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**

Progress

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

Vanson Bourne

Progress

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

Progress®

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

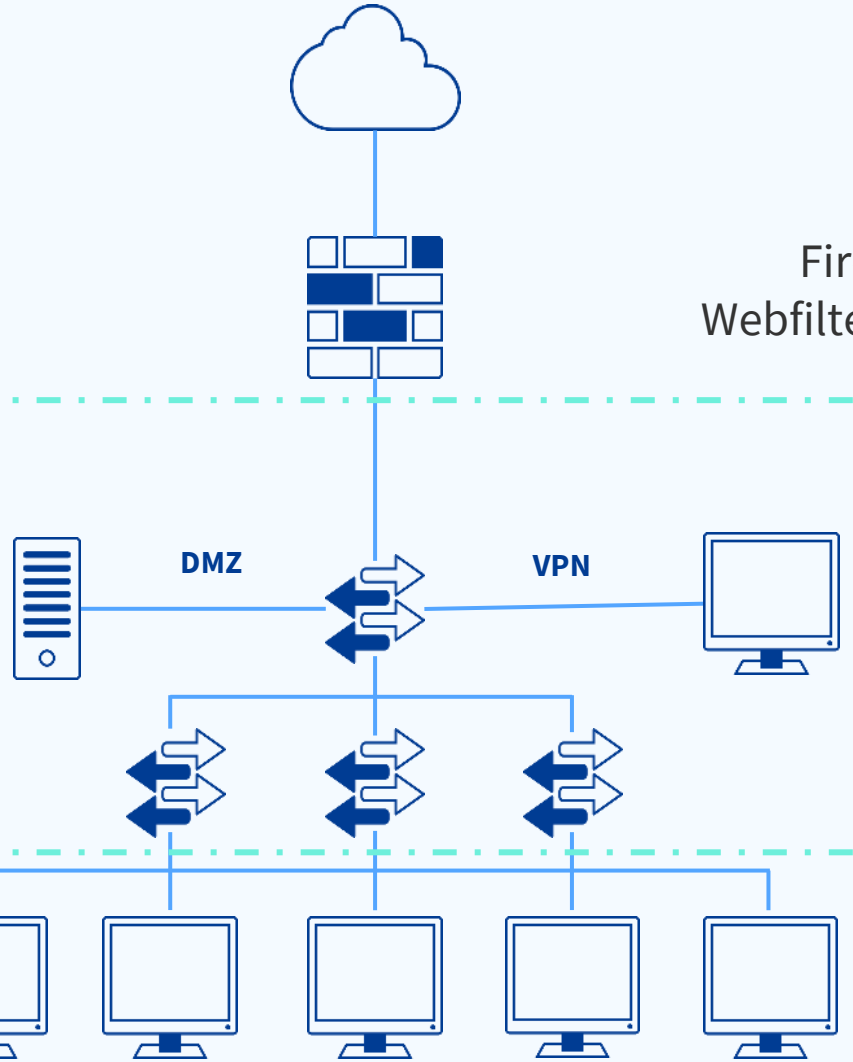
Die Angreifer verwenden fortschrittliche Techniken, um sich zu verstecken, aber sie hinterlassen dennoch überall im Netzwerk Spuren.

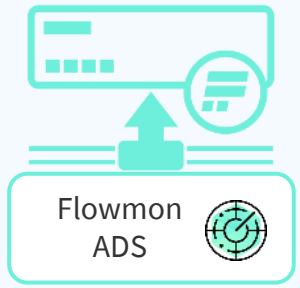
Netzwerksicherheit

✓ Perimeter-Sicherheit

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

? Netzwerksicherheit





✓ Endpunkt-Sicherheit

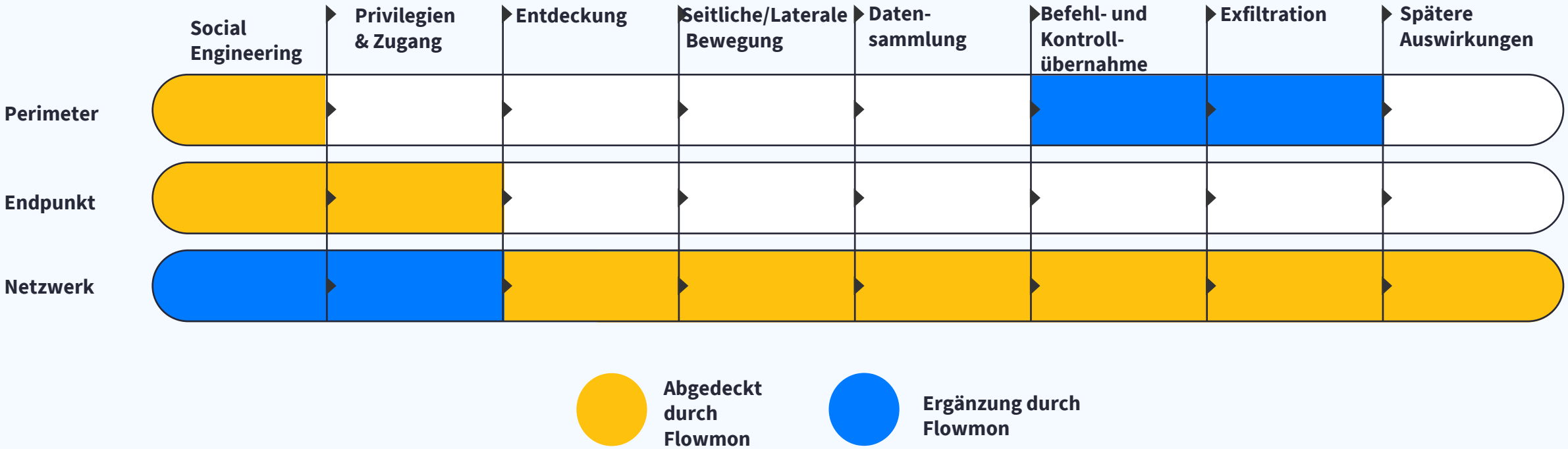
Antivirus, Personal FW,
Antimalware, Endpunkt-DLP

Gartner®

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

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

Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



Ransomware-Erkennung und -Reaktion mit Flowmon NDR

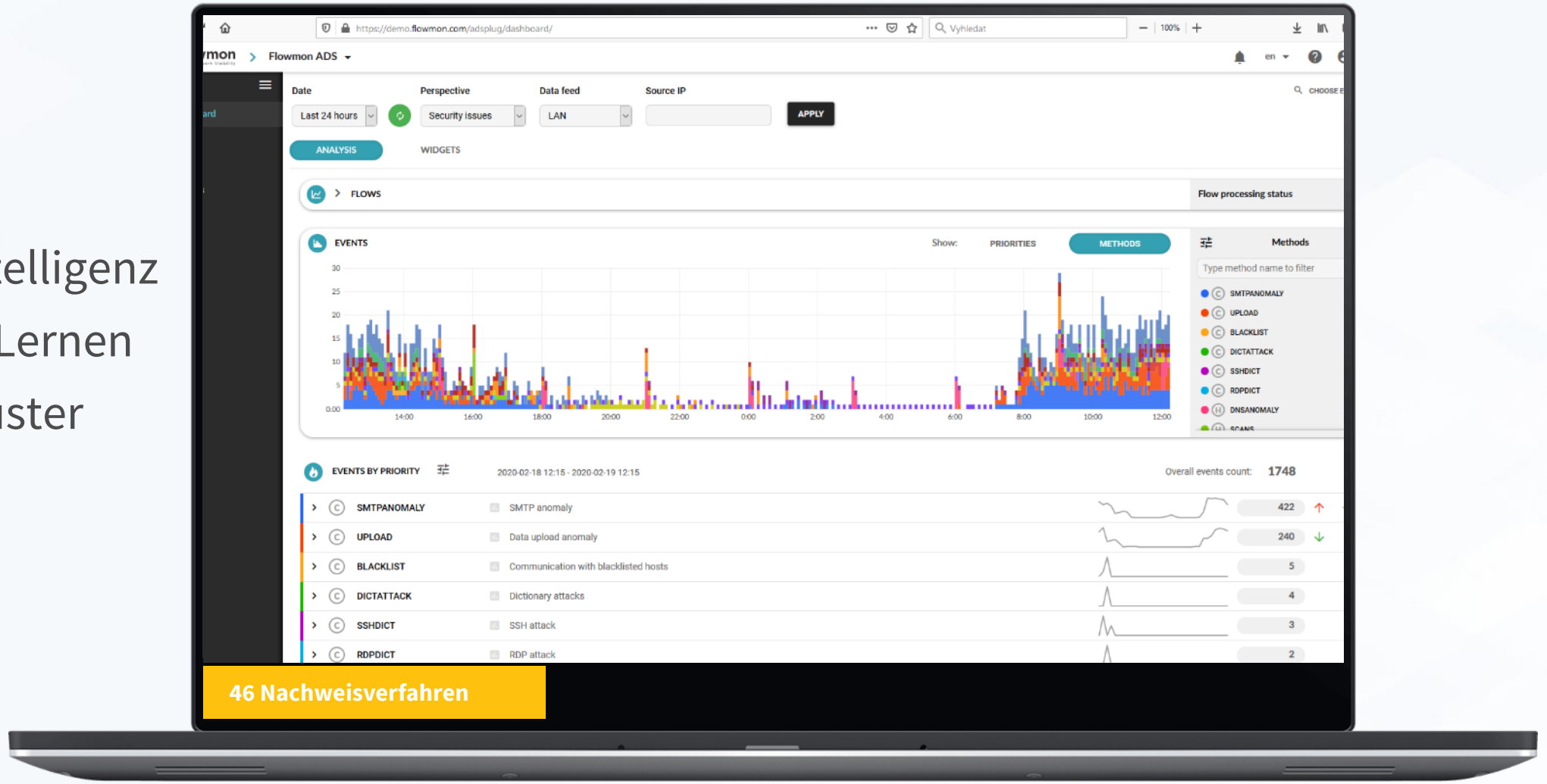
-

Anwendungsfall

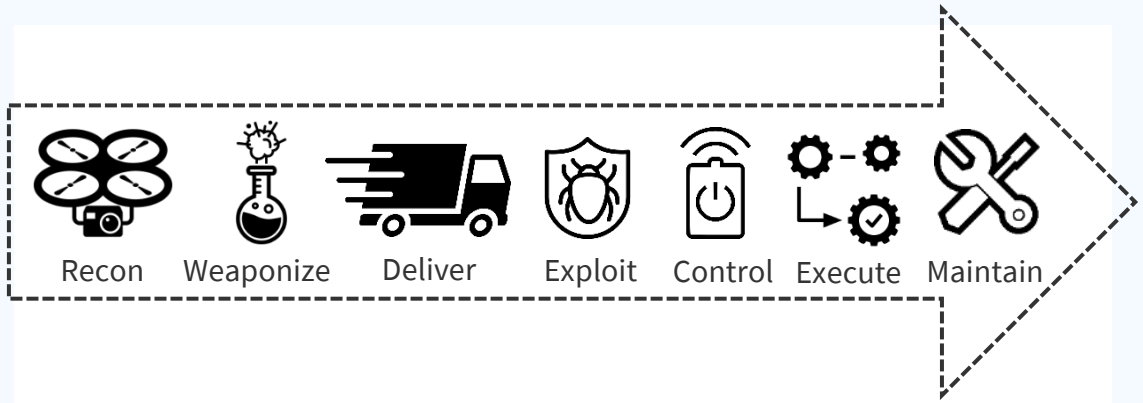
Progress | Flowmon

Flowmon Anomalie-Erkennungssystem (ADS)

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



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

Inspiriert durch einen echten Kundenfall

Vollständiges Szenario in Laborumgebung nachgebildet

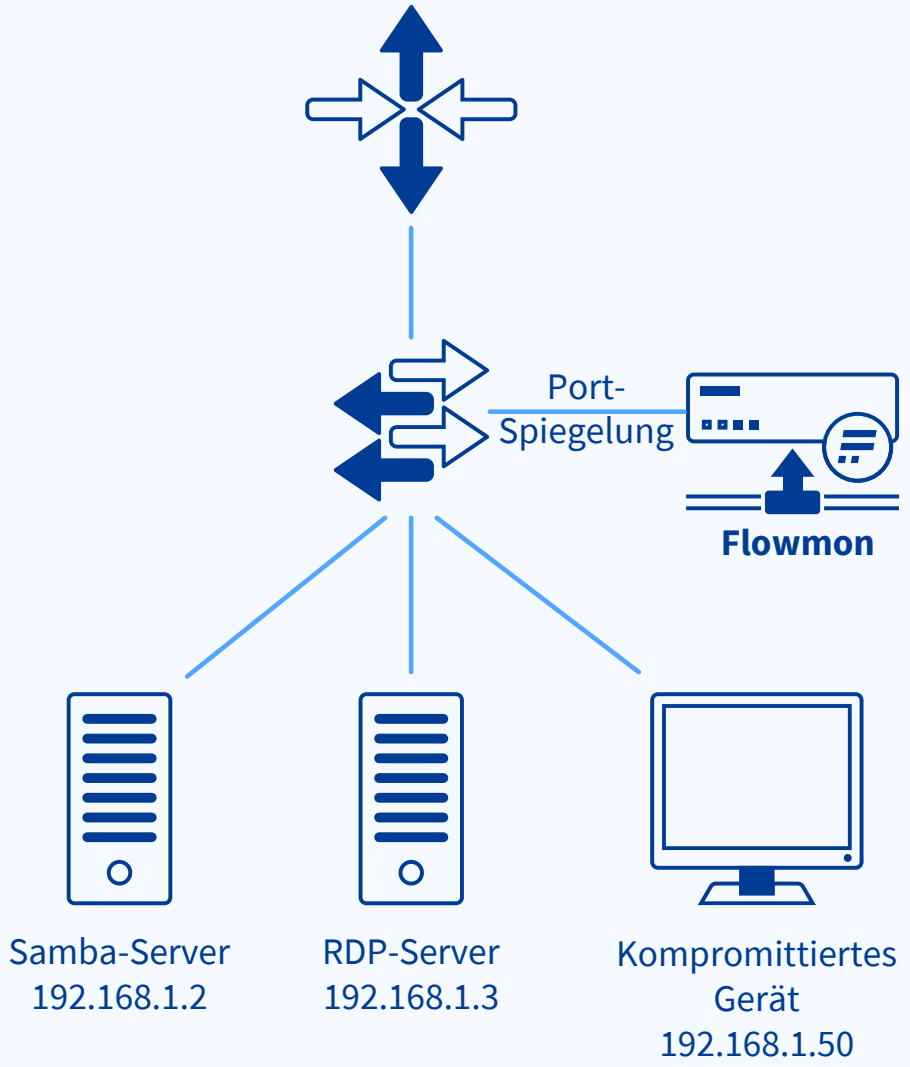
Alle Netzwerkaktivitäten werden aufgezeichnet und für Schulungszwecke zur Verfügung gestellt.

Darsteller:

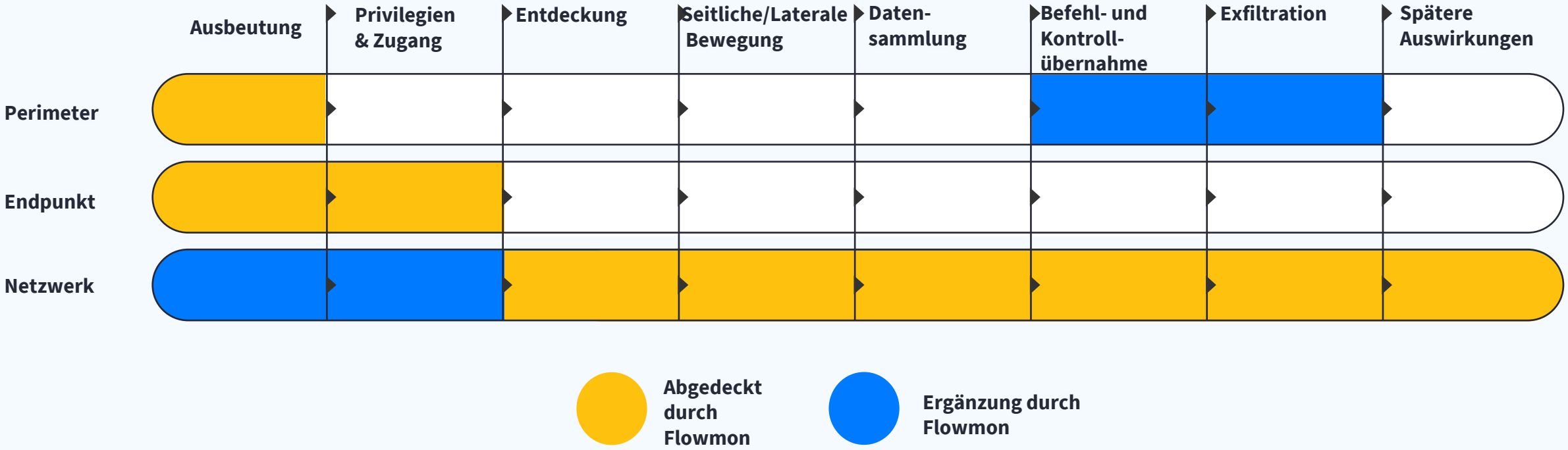
- Kompromittiertes Gerät (192.168.1.50)
- Samba-Server (192.168.1.2)
- RDP-Server (192.168.1.3)

Zielsetzungen:

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

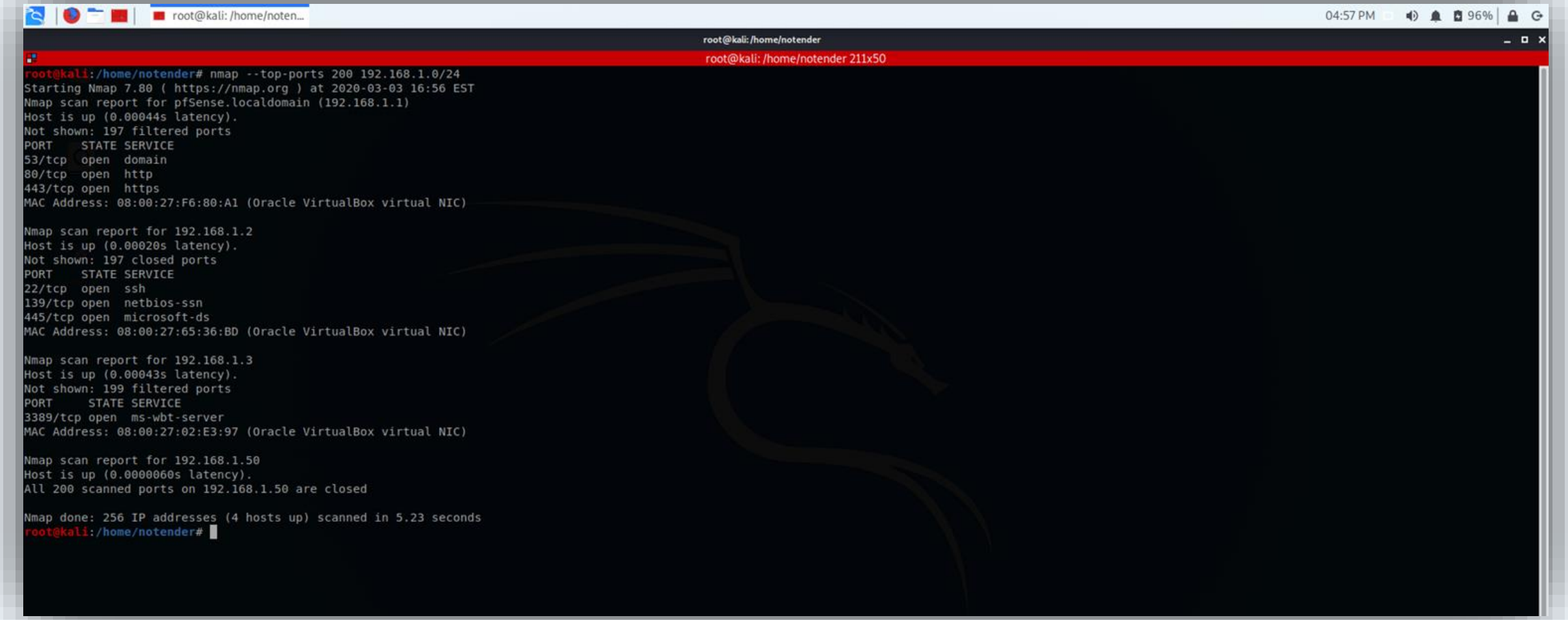


Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



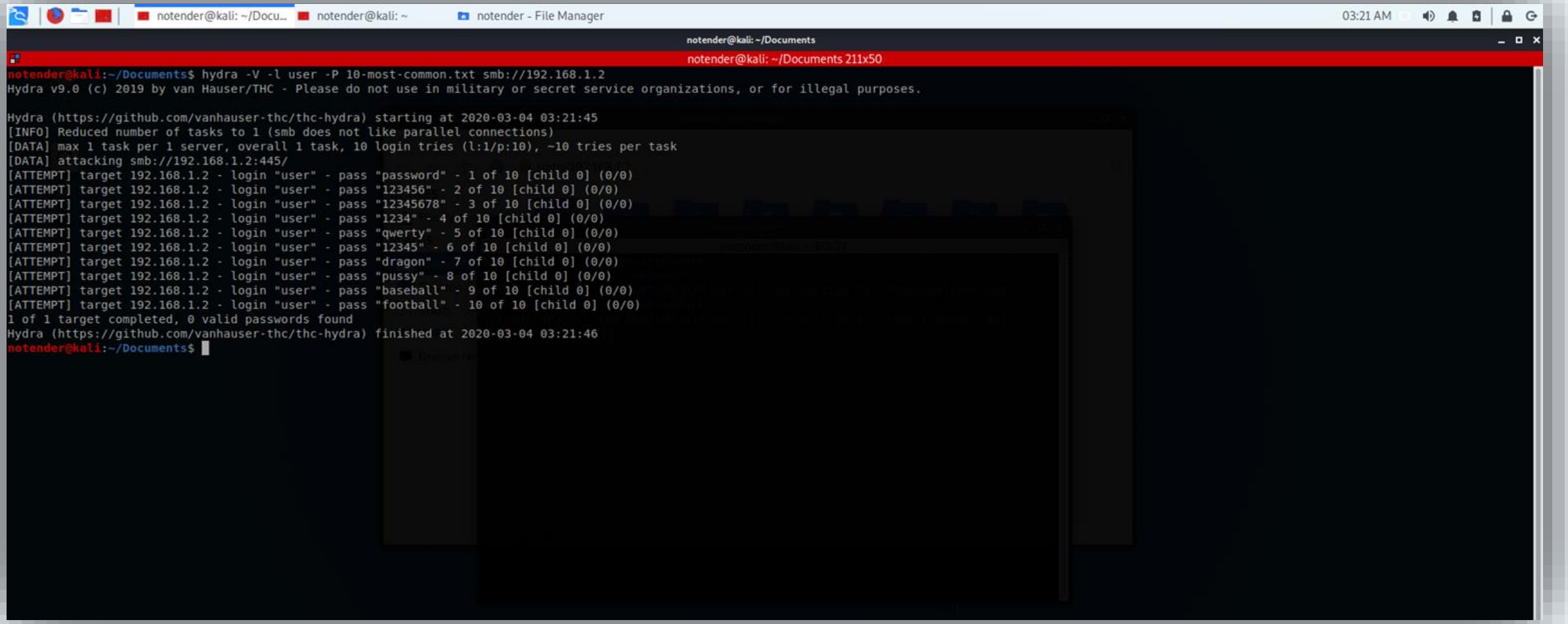
Entdeckung

Böser Akteur auf der Suche nach Zielen



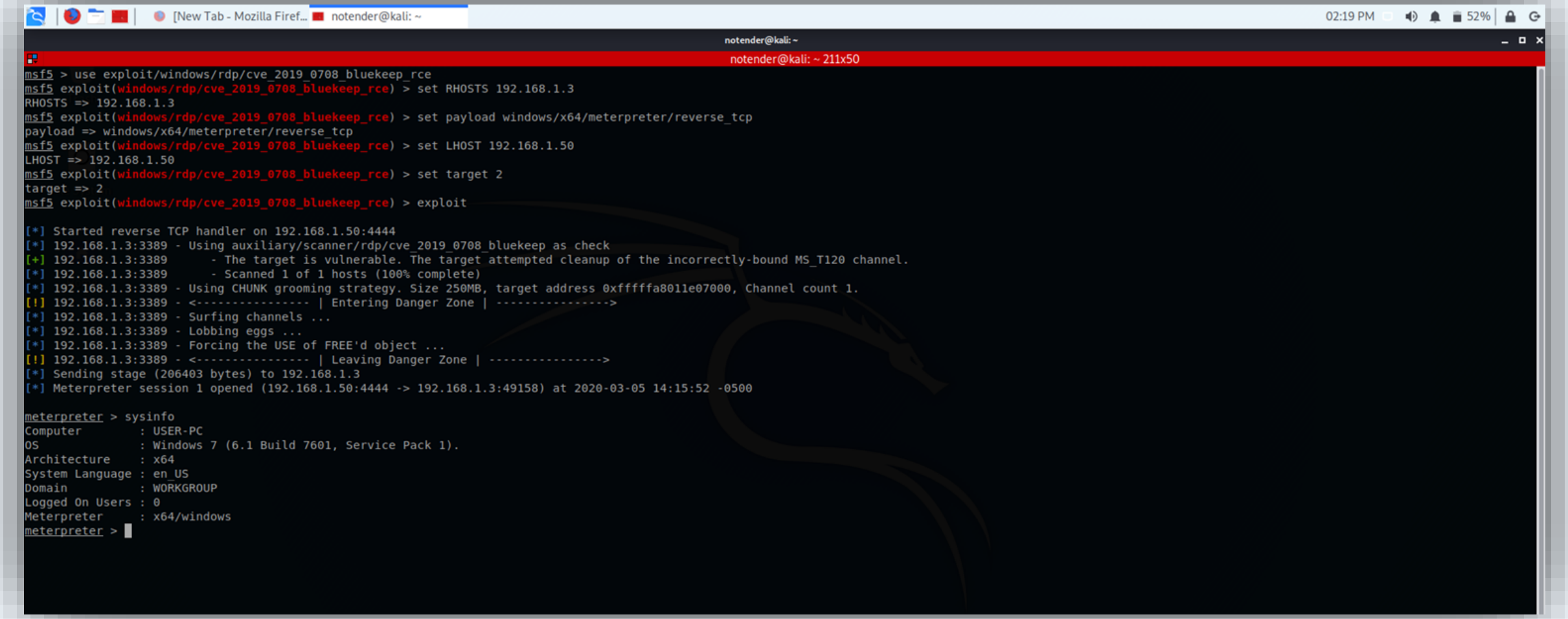
Zugang zu Anmeldeinformationen

Passwort-Spraying gegen Samba-Server



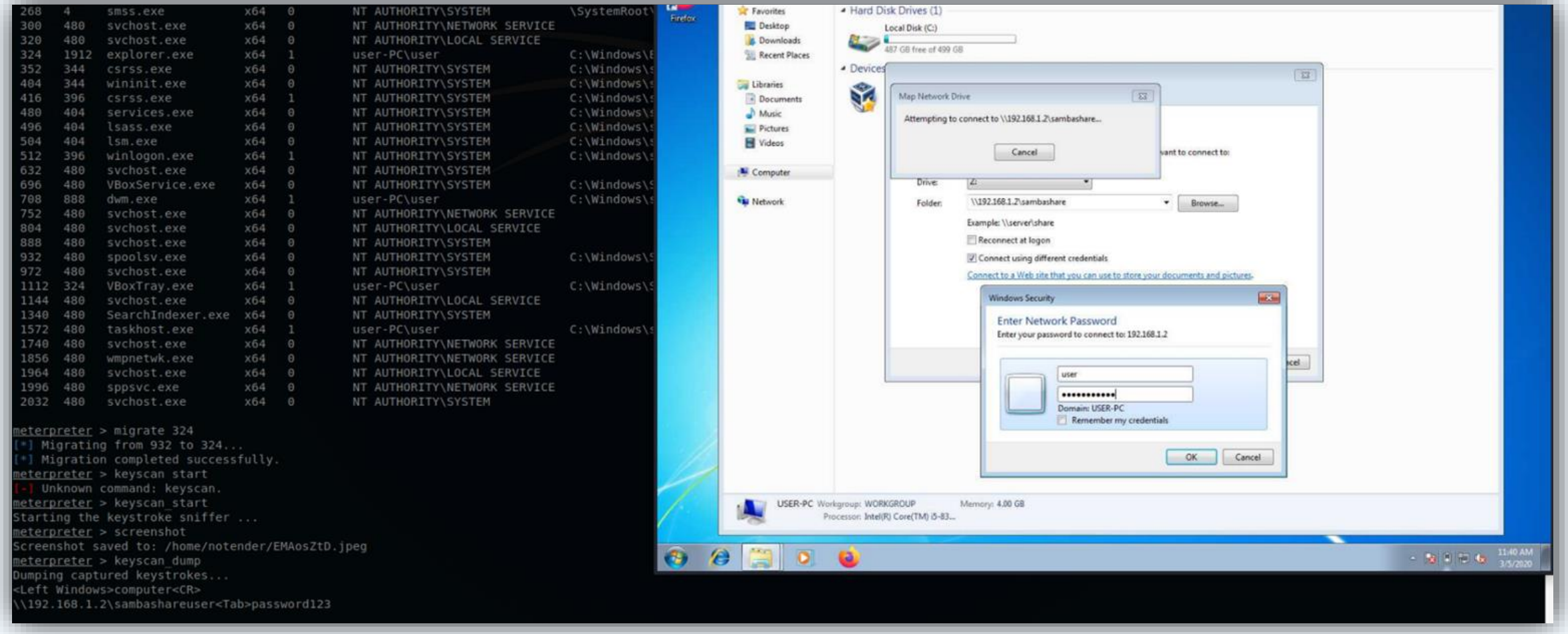
Seitliche Verschiebung

Angreifer nutzte Schwachstelle im RDP-Protokoll Bluekeep aus



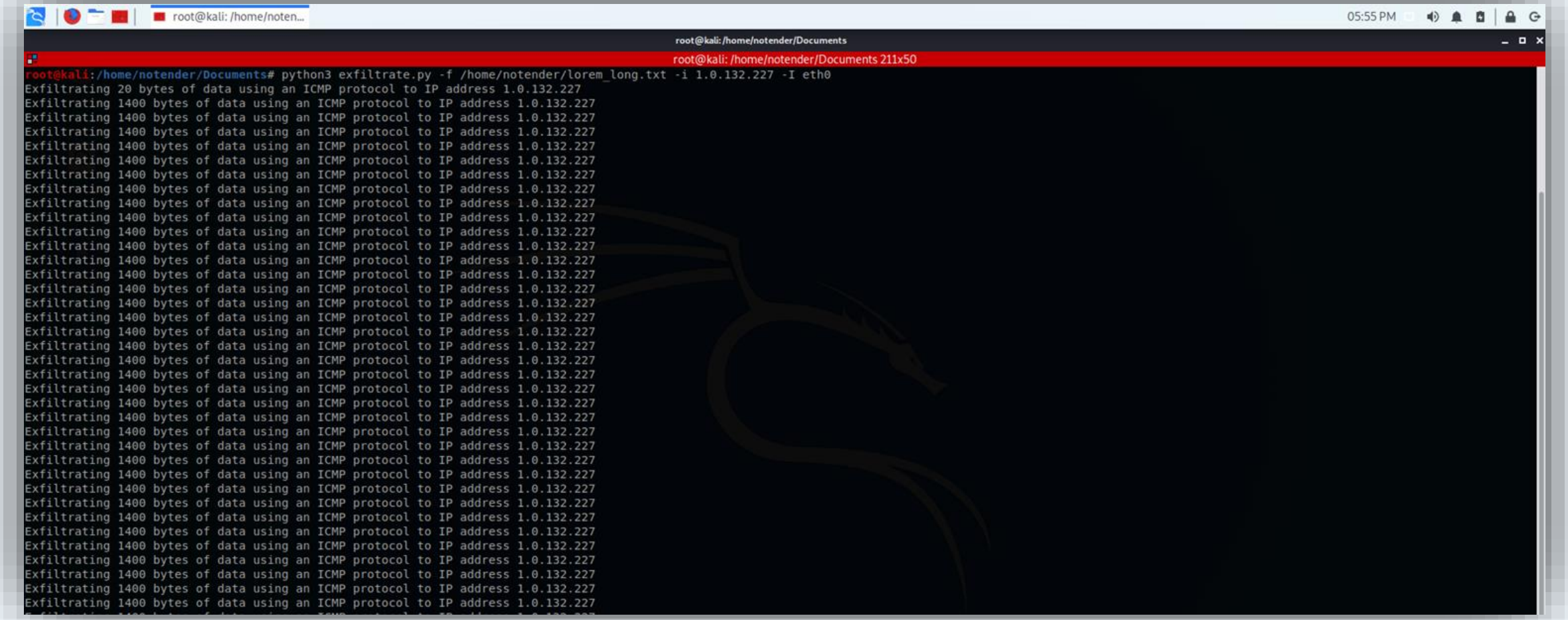
Eingabe-Erfassung

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

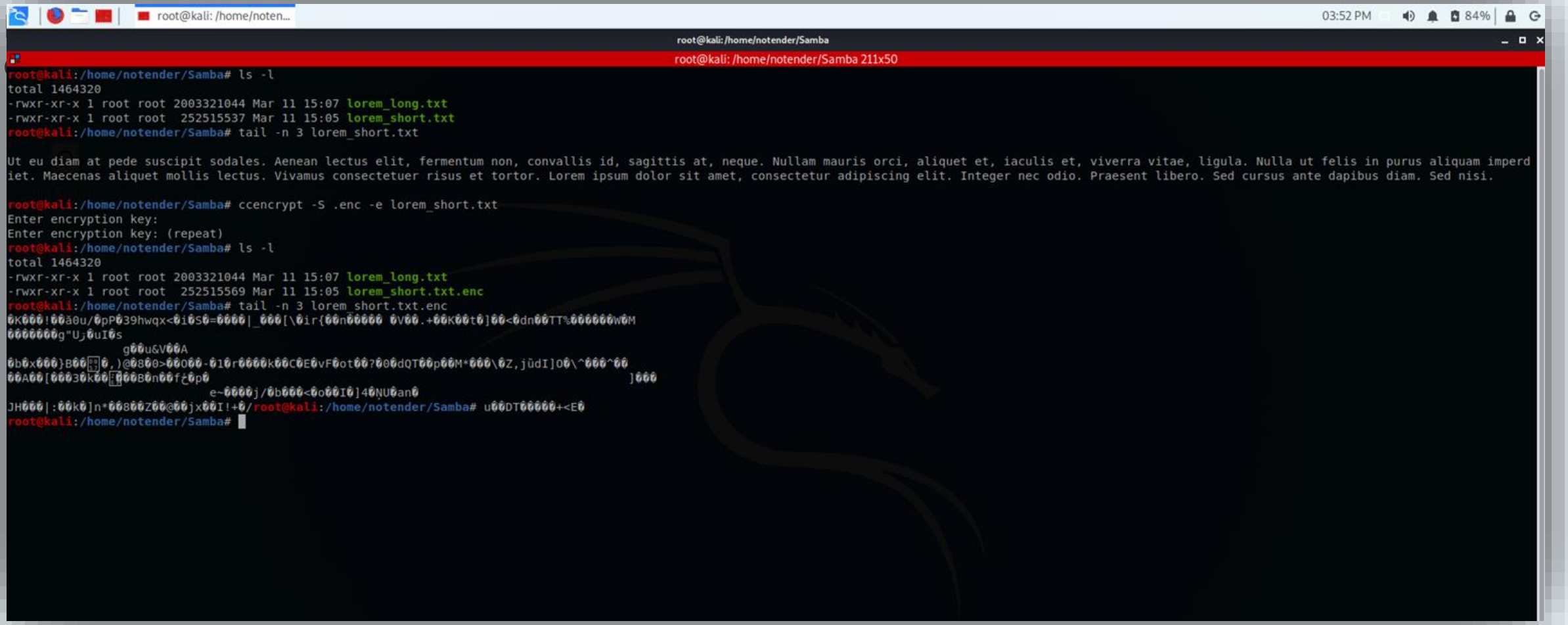


Datenexfiltration

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

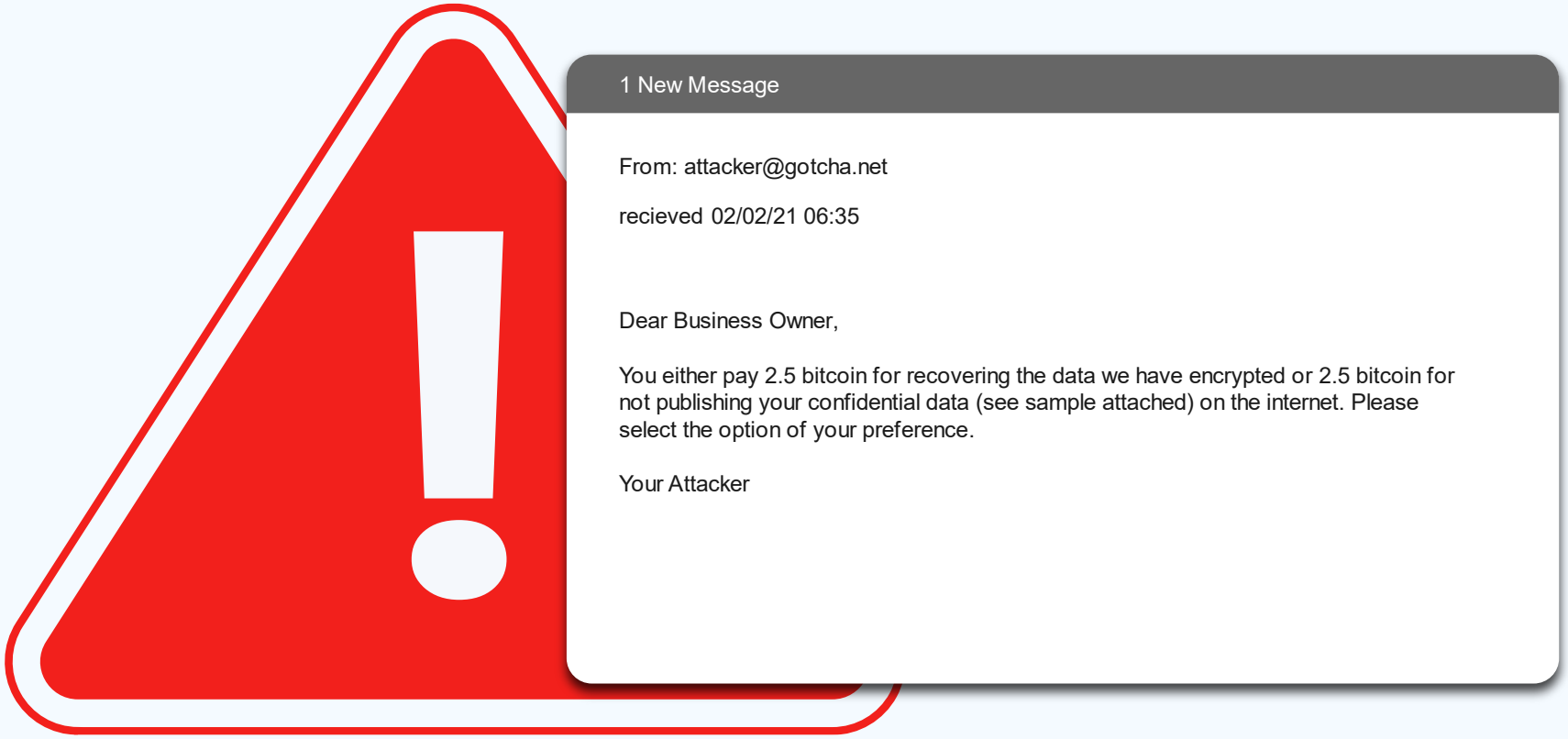


Die letzten Schritte des Angriffs werden inszeniert

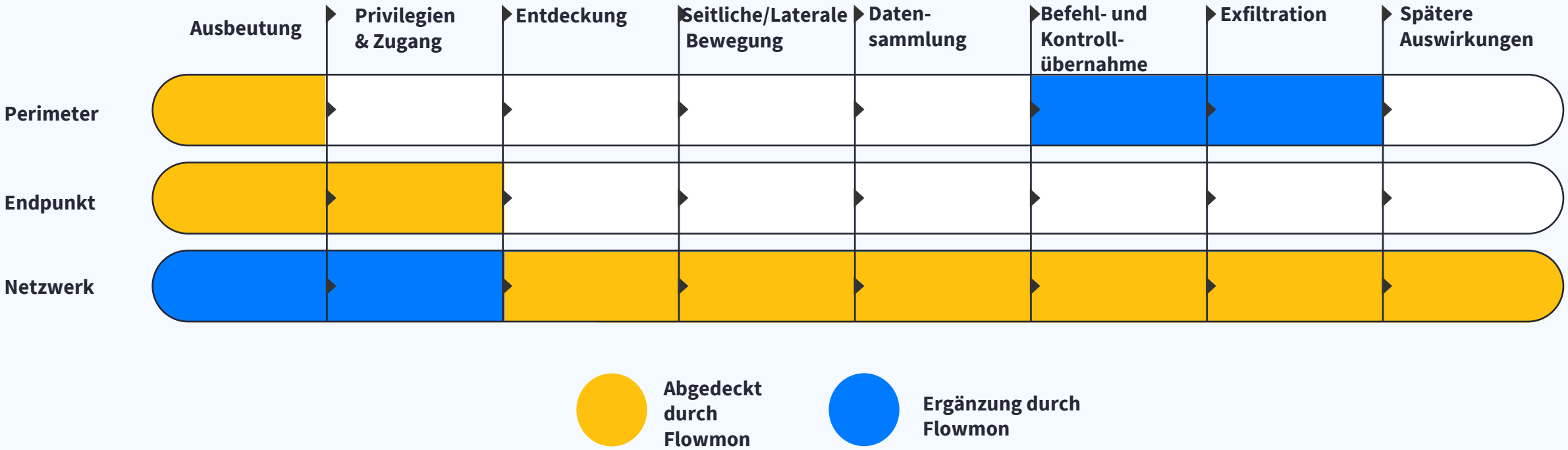


Ergebnisse bei Nicht-Erkennung

Mögliche öffentliche Exposition

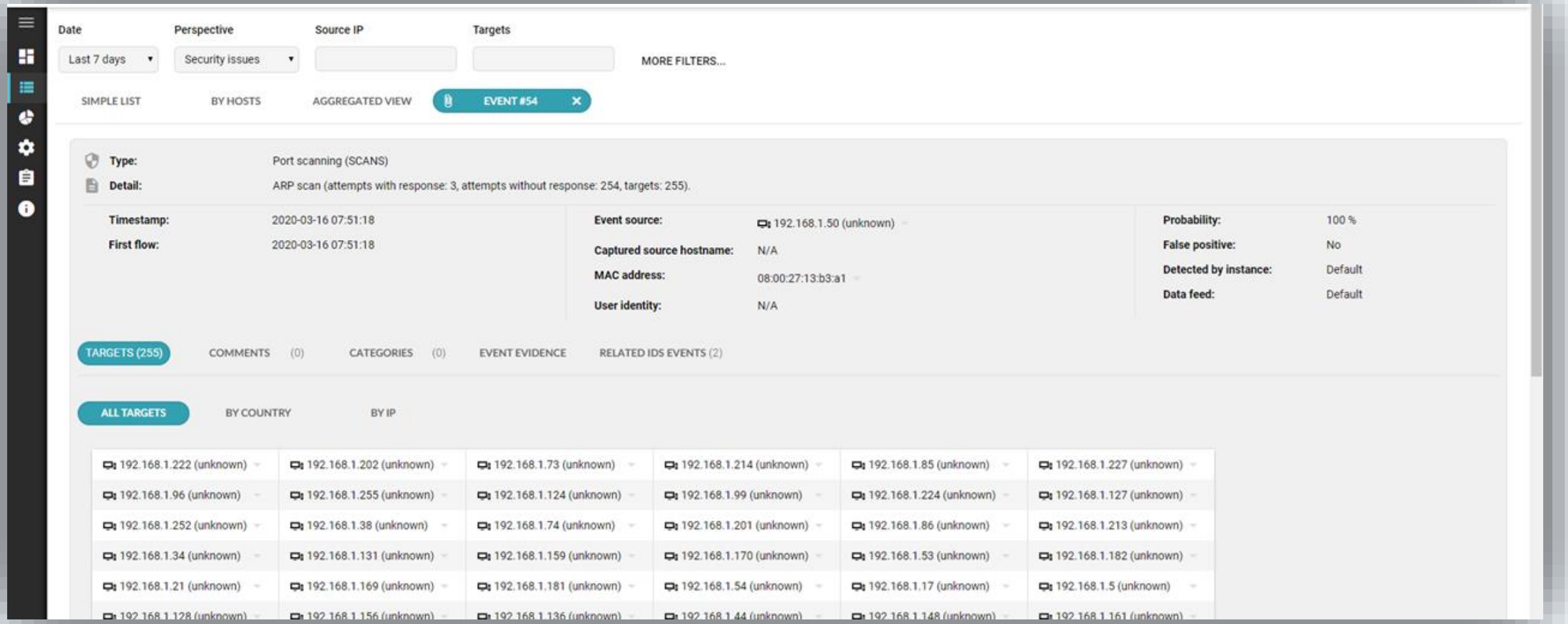


Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



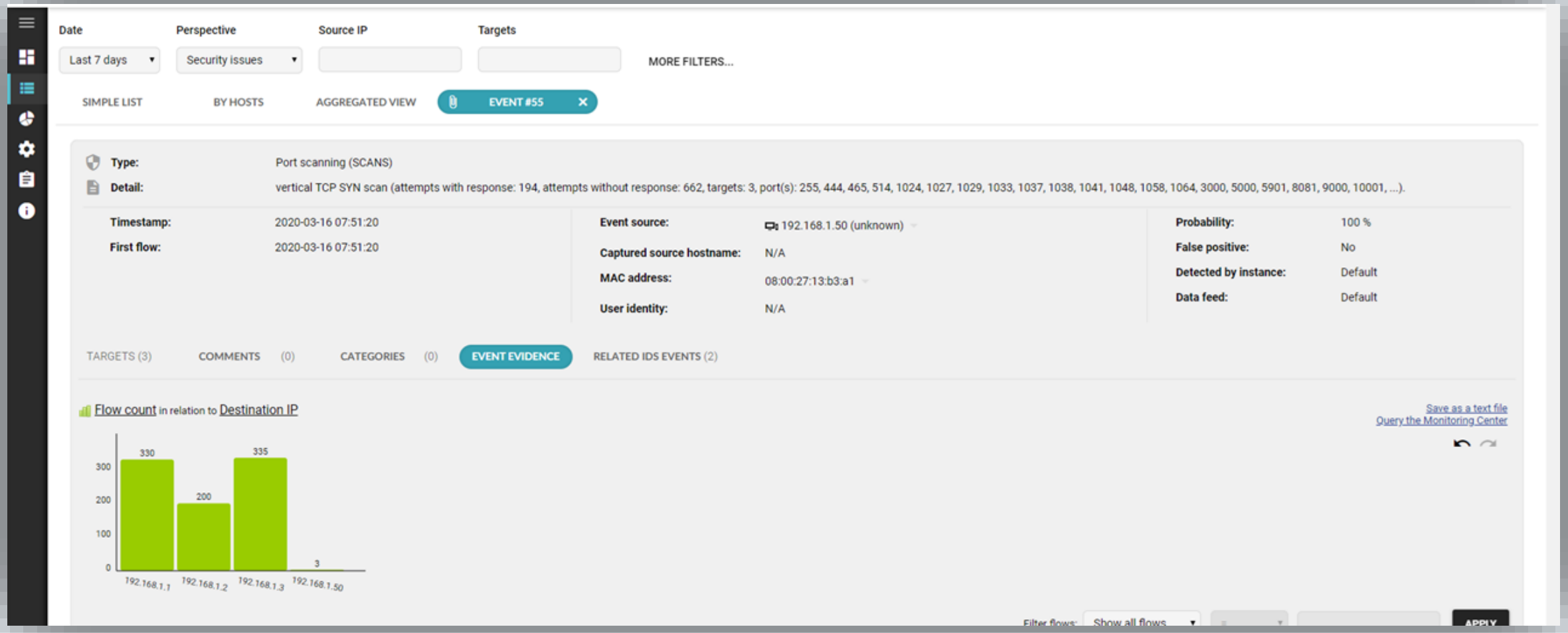
ARP-Scan

Quelle 192.168.1.50, Aufzählung der aktiven Nachbar-Hosts im Netz

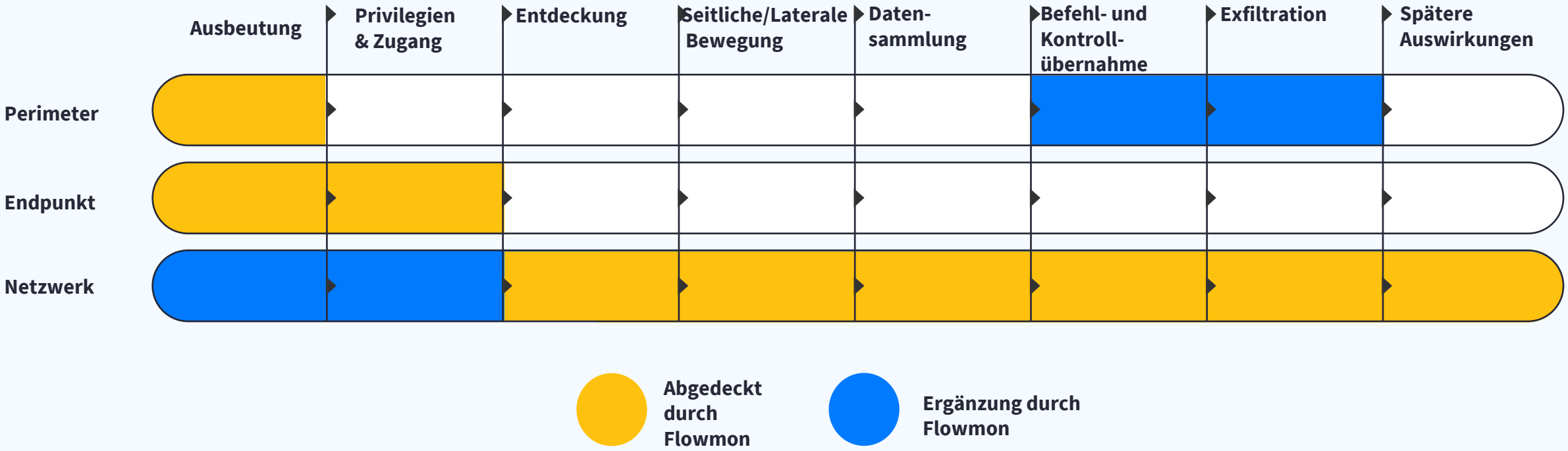


Vertikaler TCP SYN

Scan gegen 3 entdeckte Ziele, um ausnutzbare Dienste zu finden

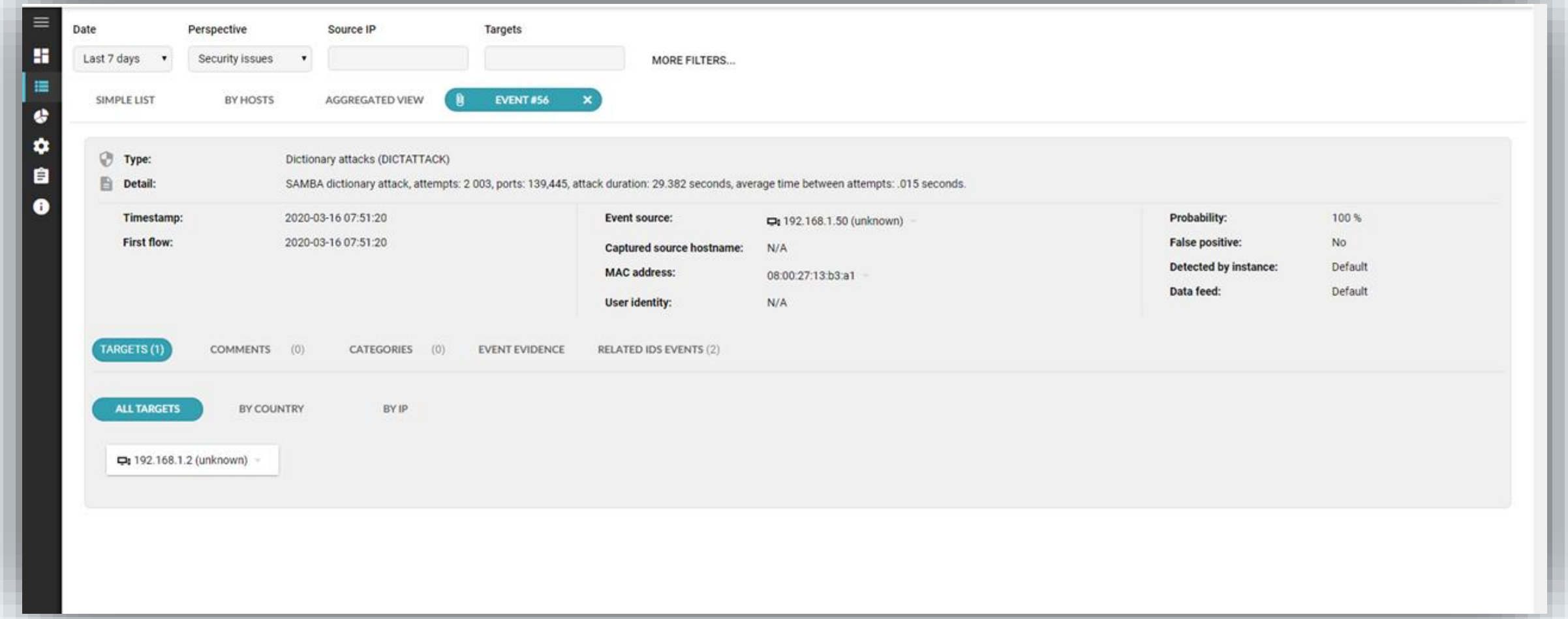


Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



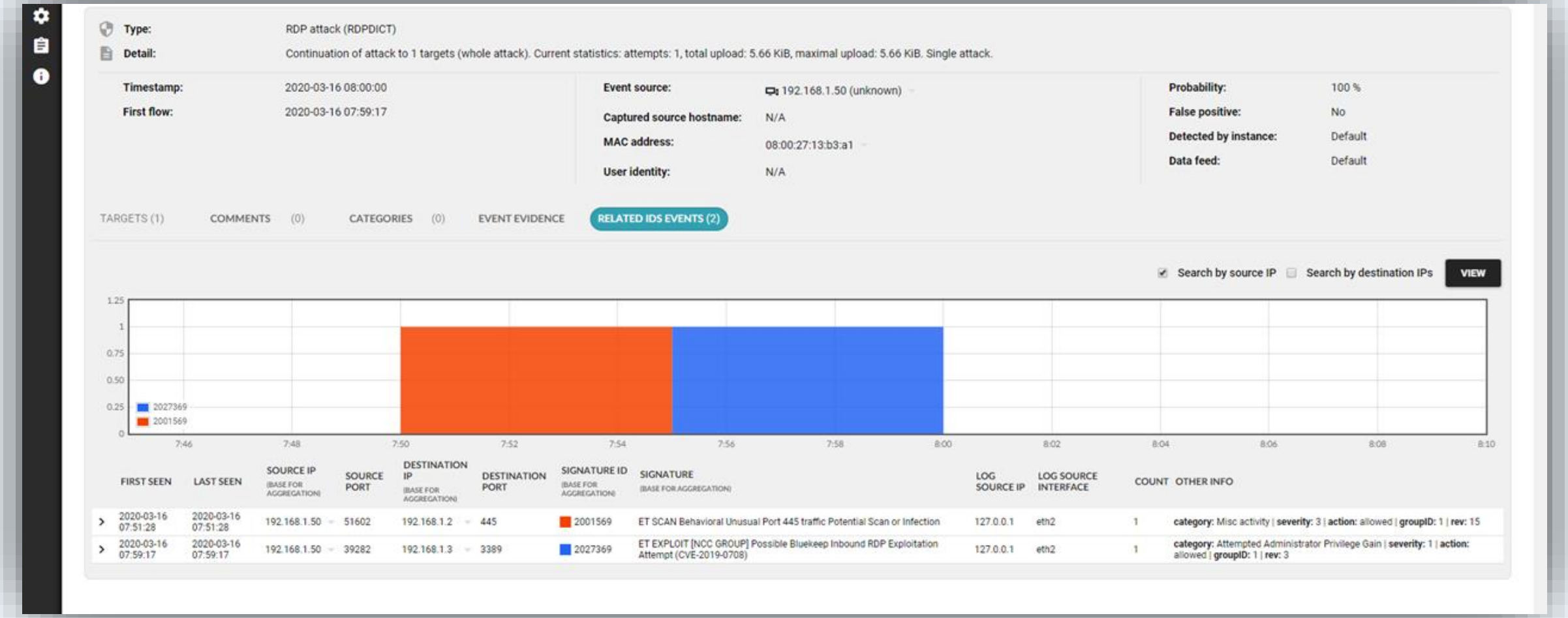
Samba Brute-Force-Angriff

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

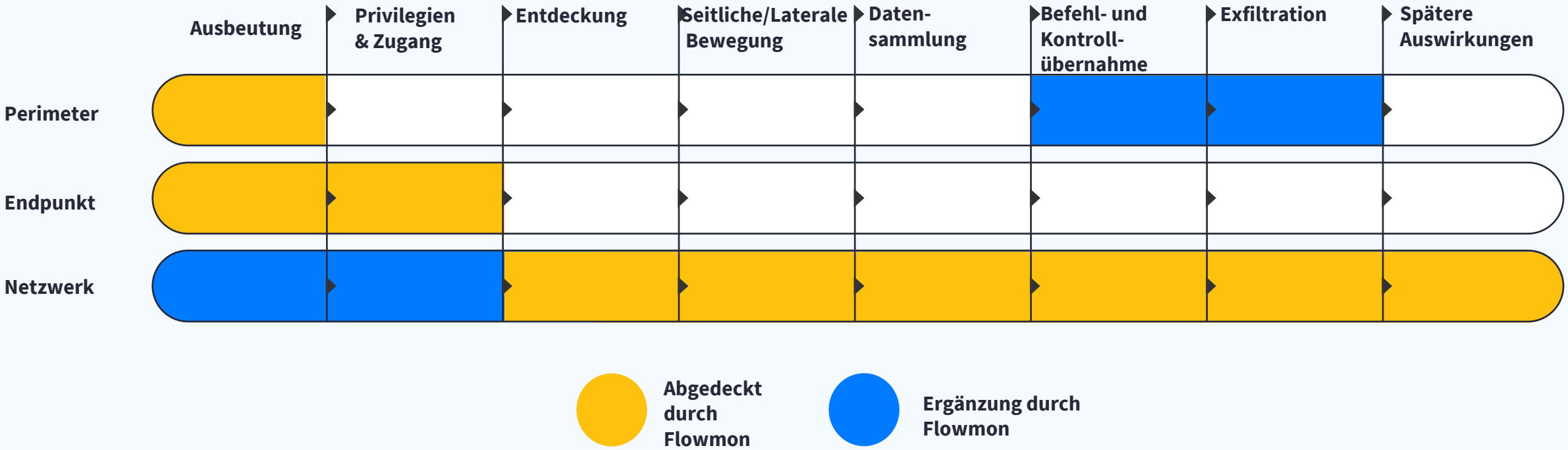


Erkennung von Eskalationen

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

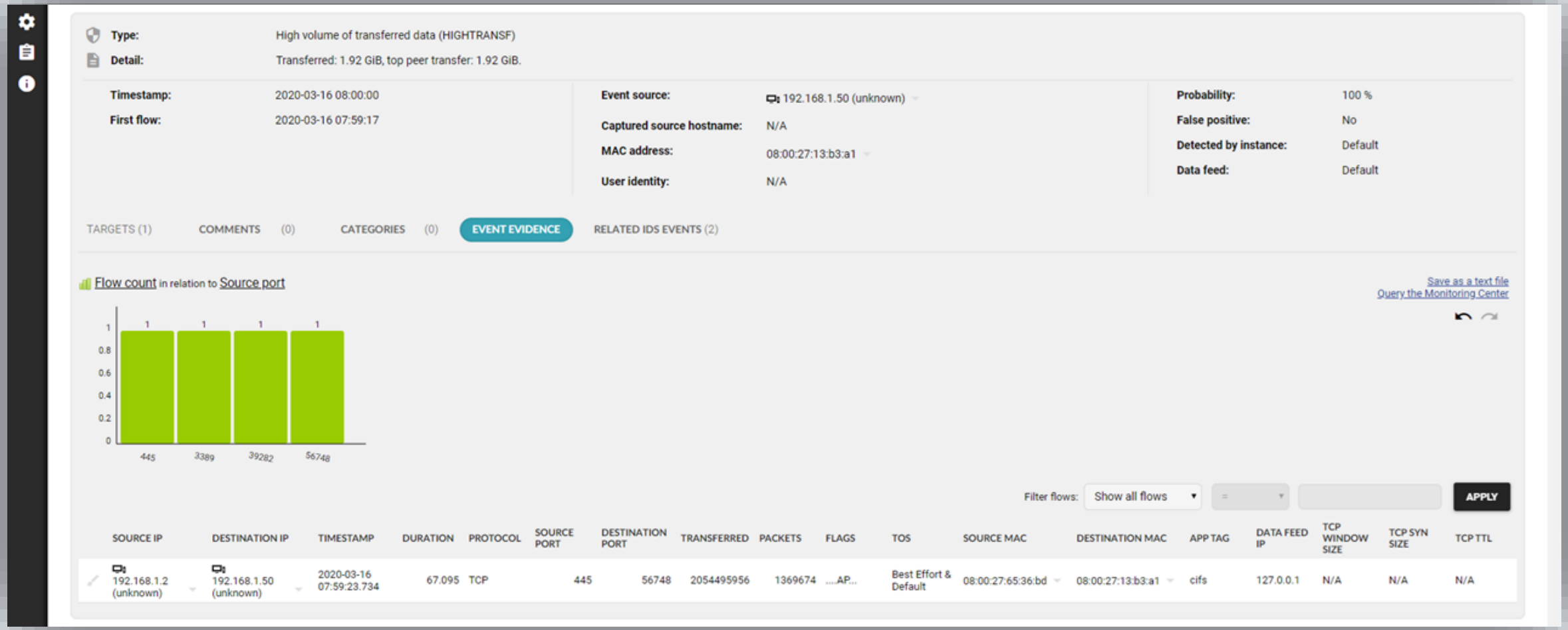


Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework

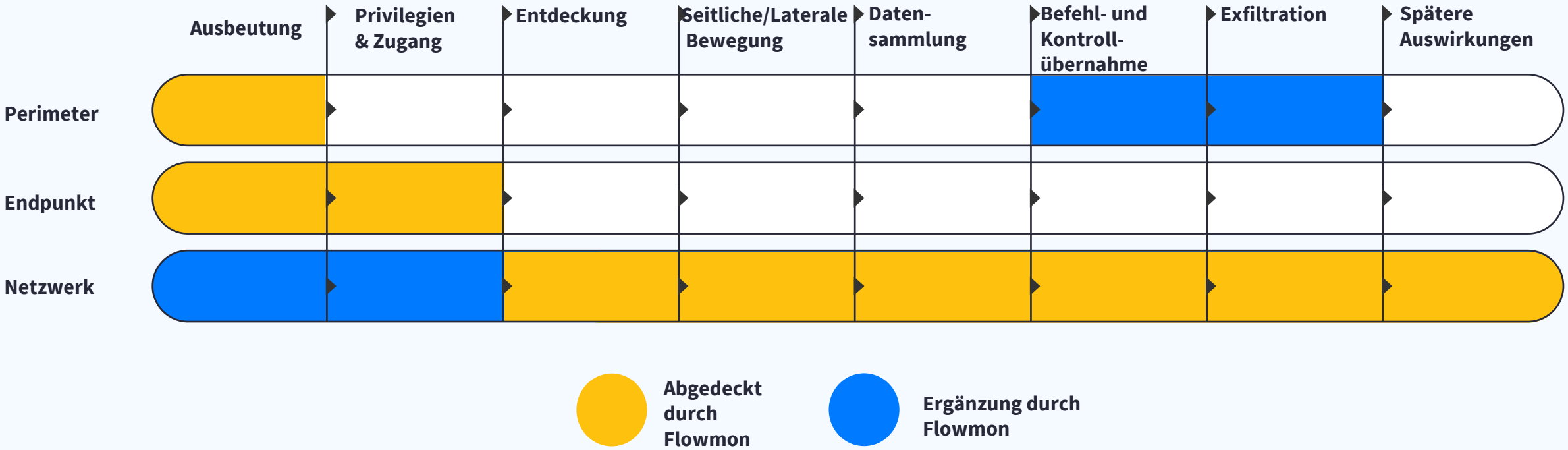


Hoher Datentransfer festgestellt

Angreifer beginnt, sensible Unternehmensdaten vom Server 192.168.1.2 zu exfiltrieren

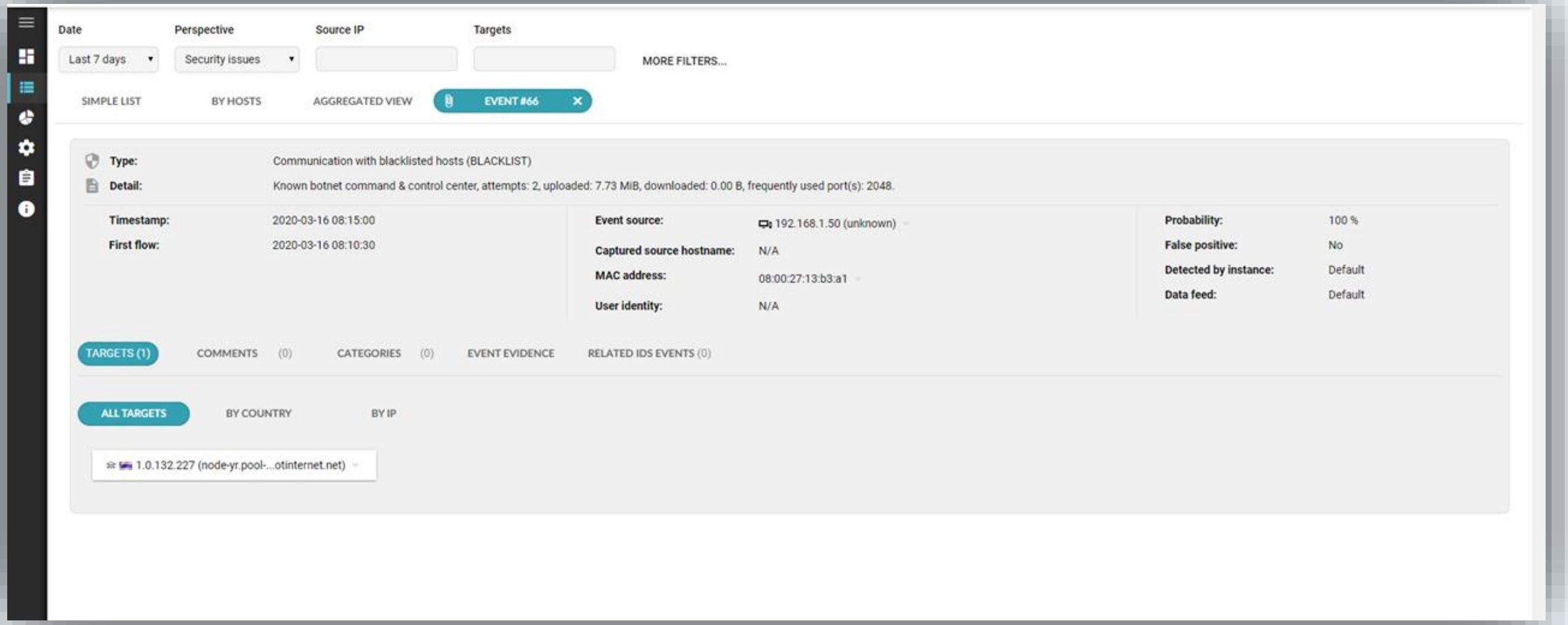


Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework

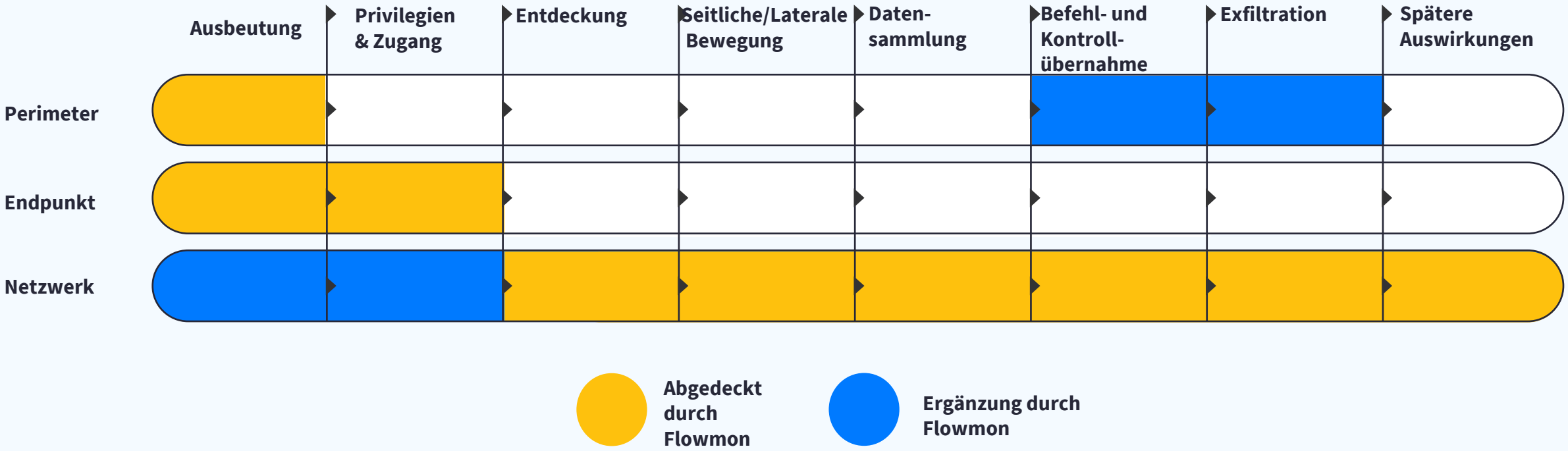


Botnet Command and Control

Erkennung der Kommunikation anhand von Indikatoren für eine Kompromittierung

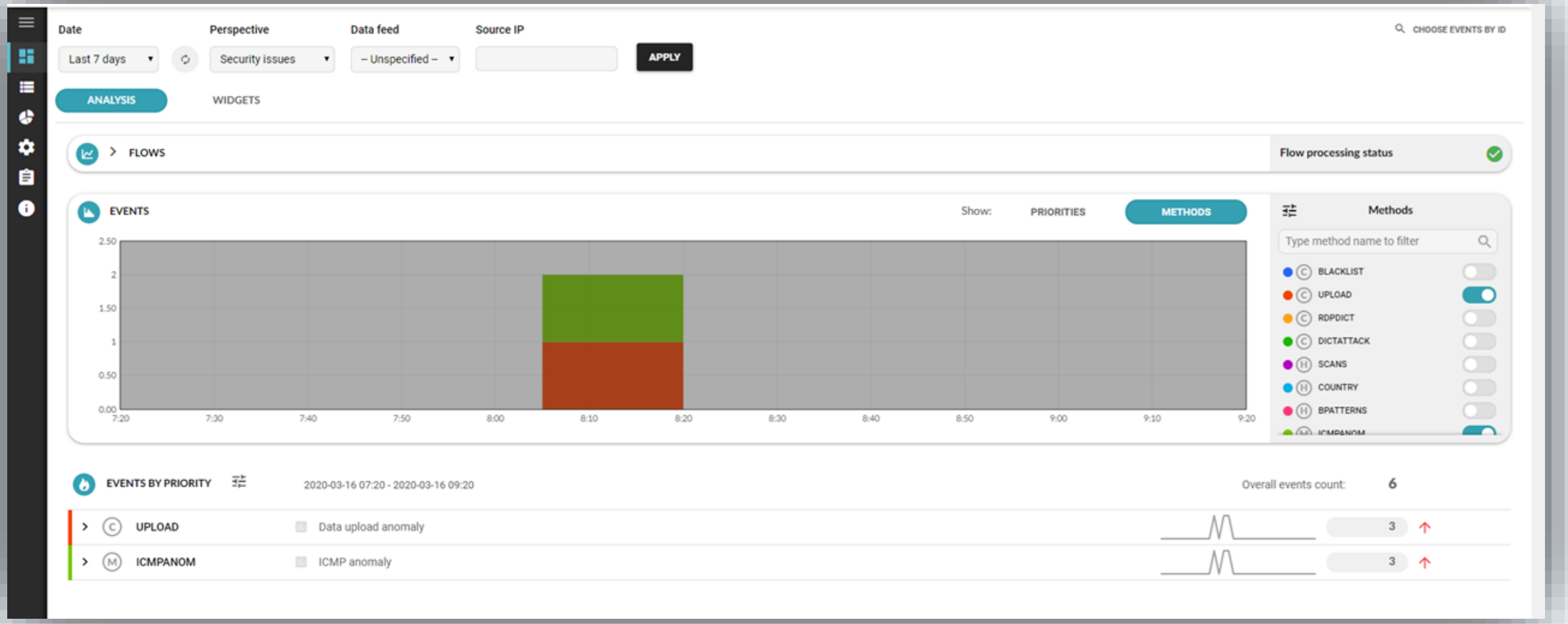


Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework



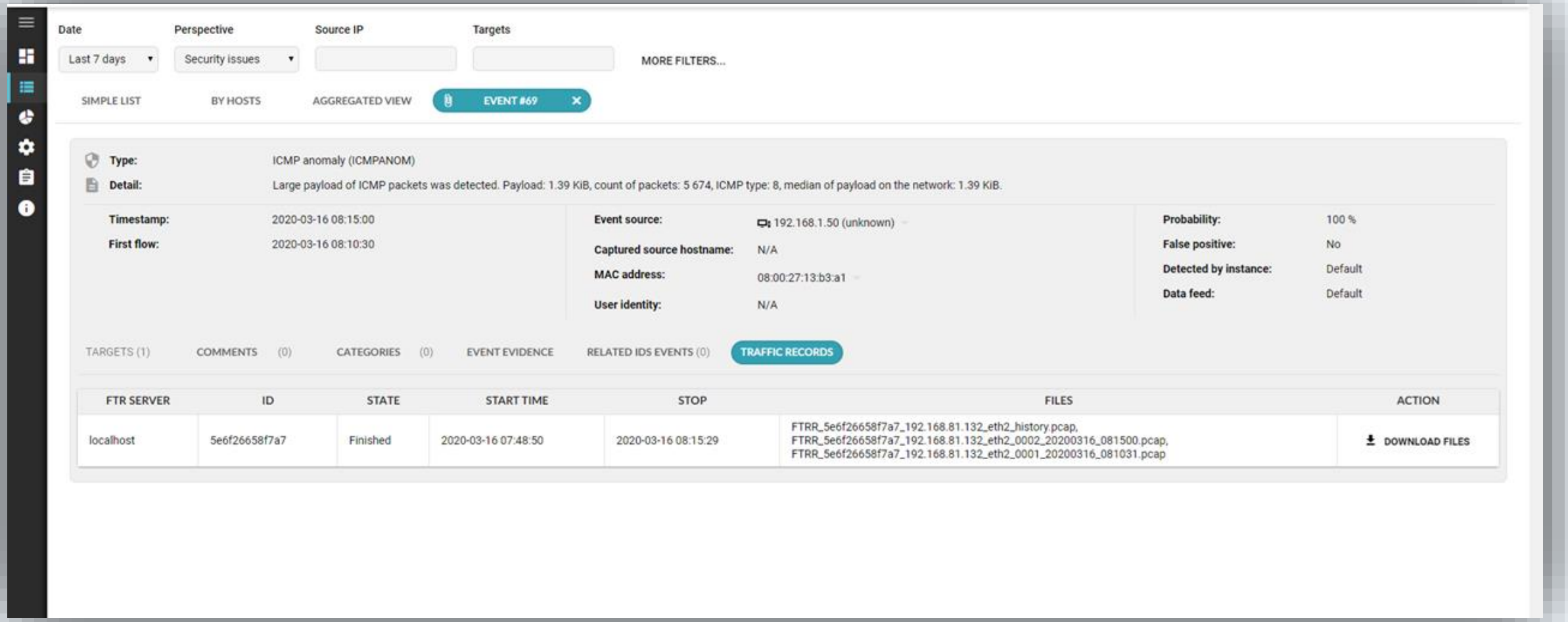
Signale für anomales Verhalten

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



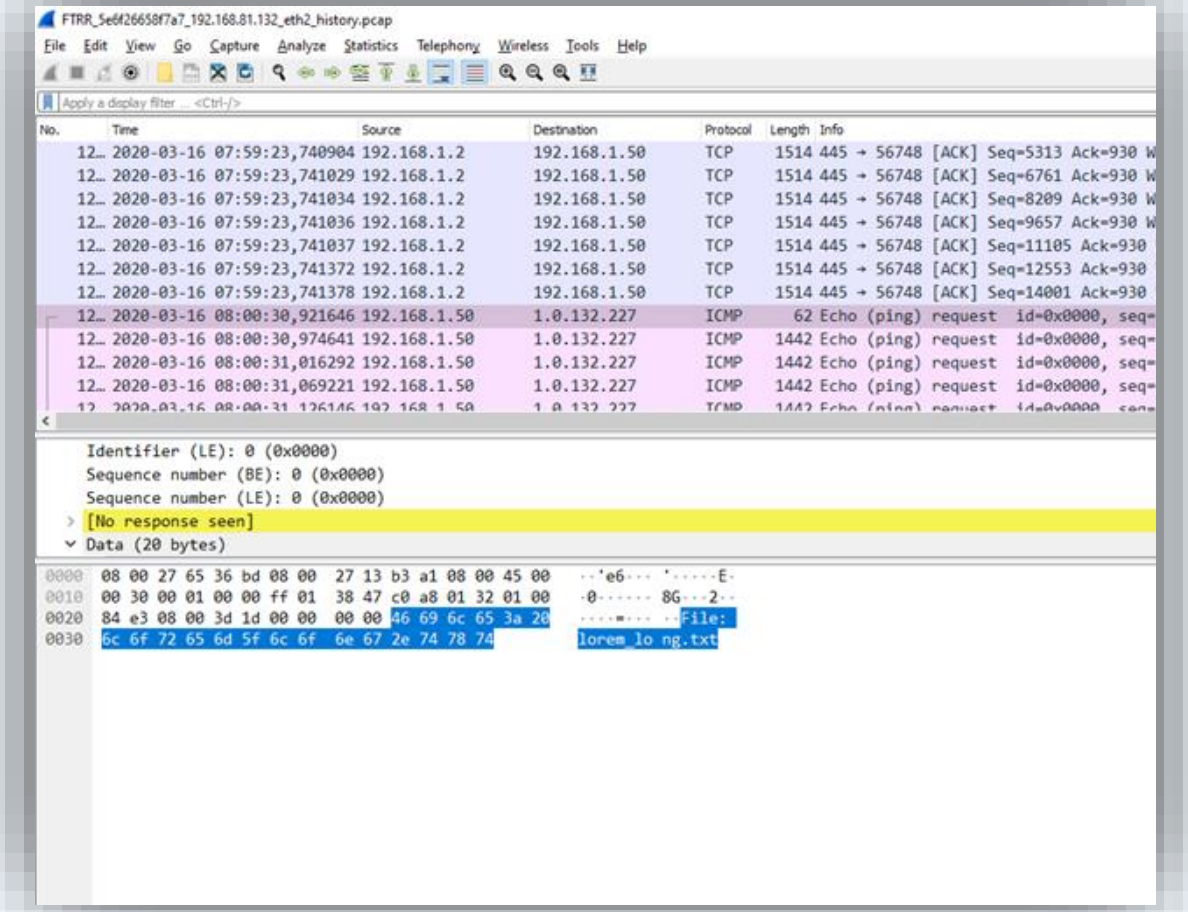
Erkennung verdächtiger Nutzdaten

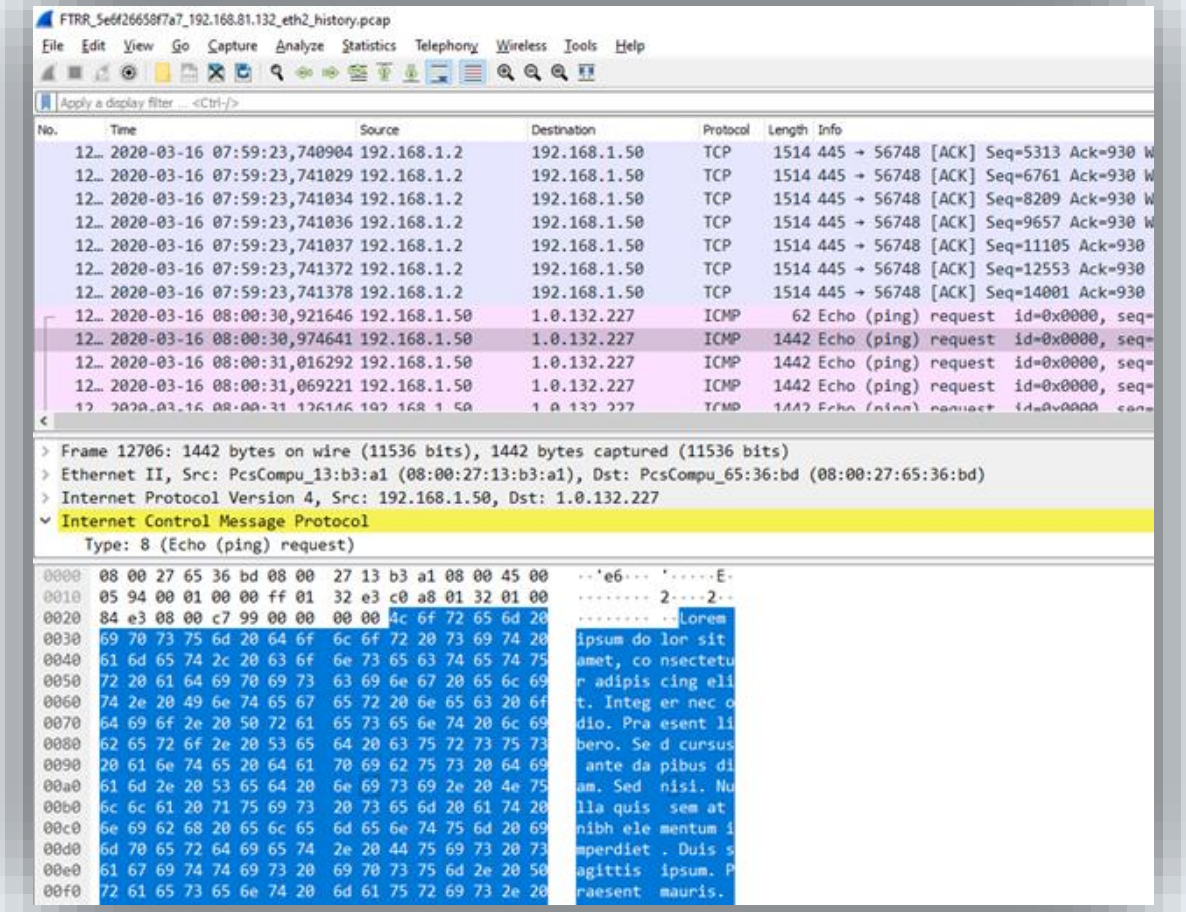
Erkennung von ICMP-Paketen mit verdächtiger Nutzlast, die automatisch eine vollständige Paketverfolgung auslösen



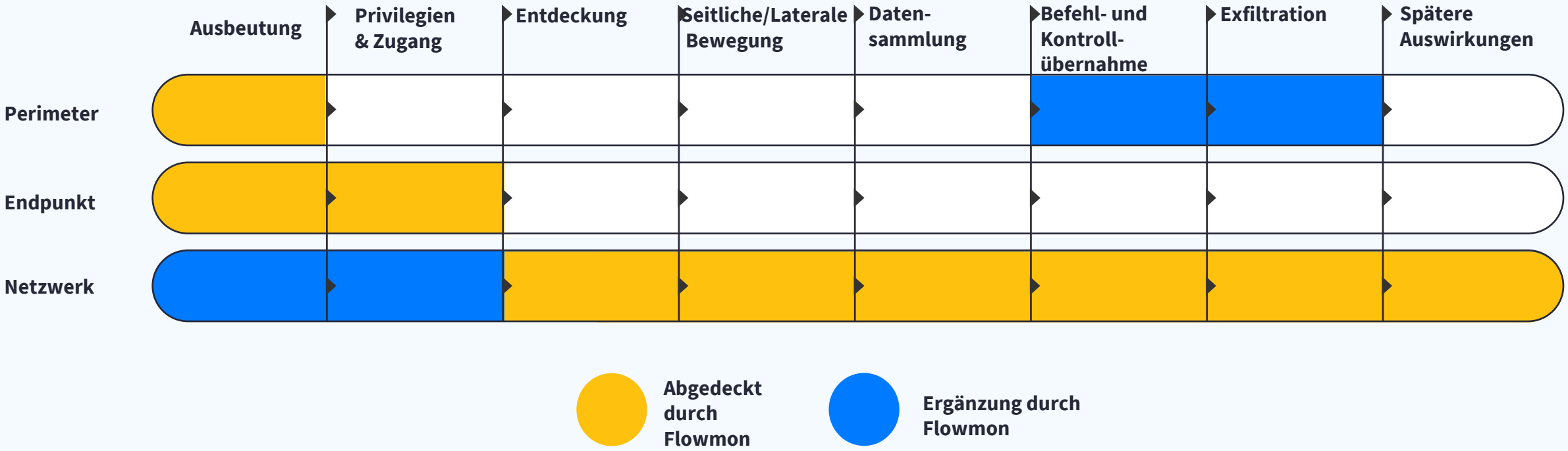
Exfiltrierte Dateidaten

Vollständige Paketverfolgung mit dem Namen und Inhalt der exfiltrierten Datei



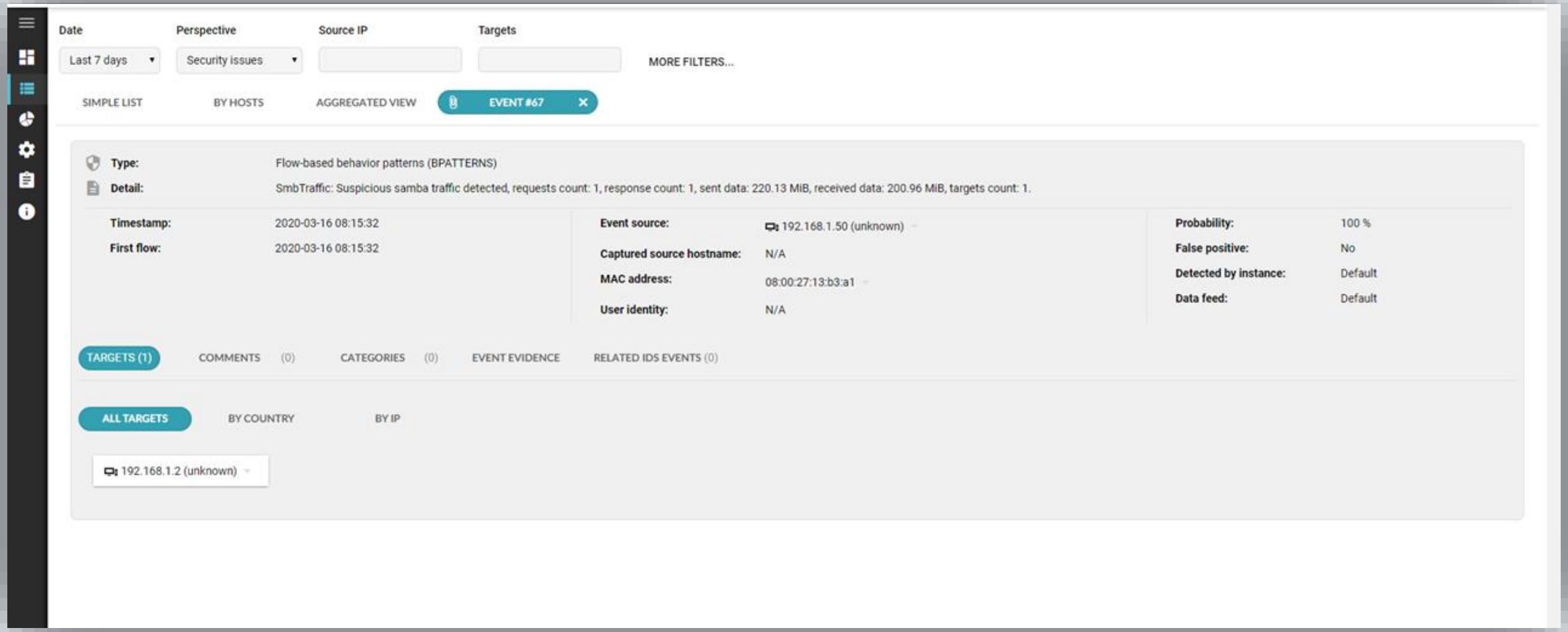


Mehrschichtige Sicherheit durch Nutzung des MITRE ATT&CK Framework

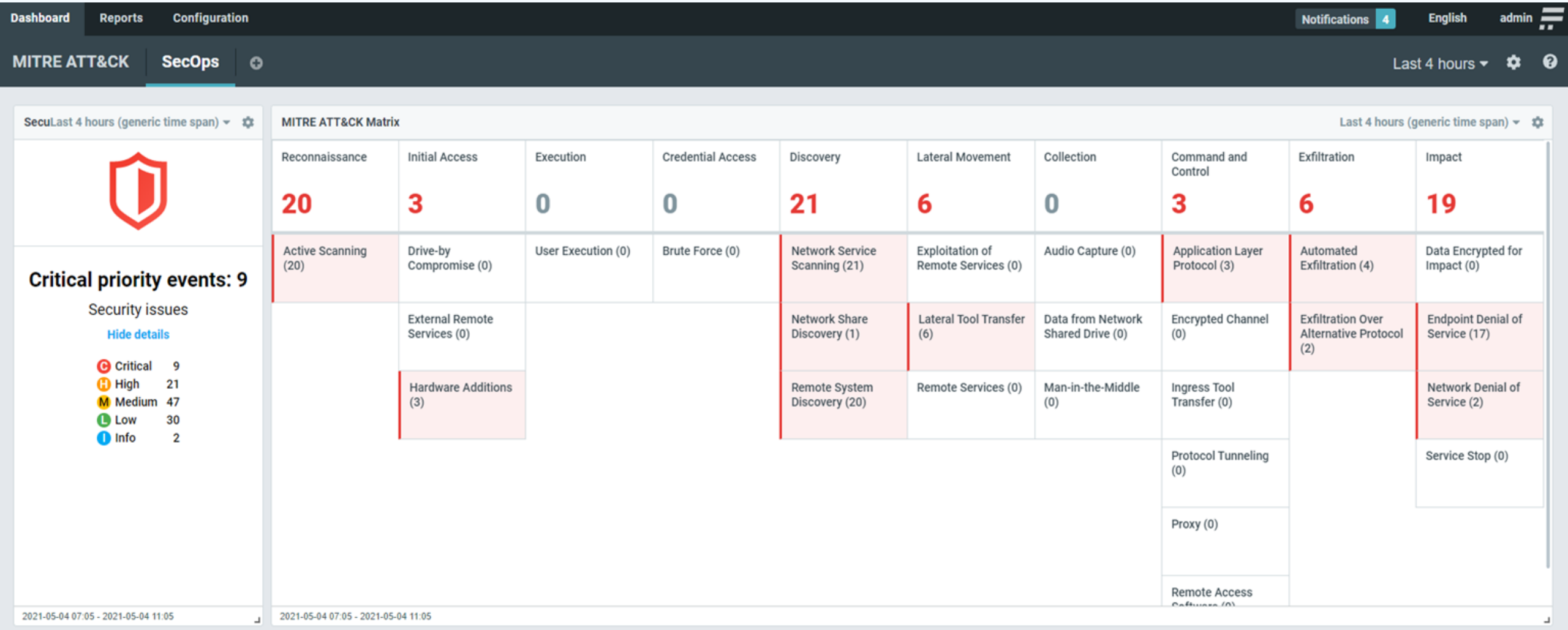


Verdächtiger Samba-Datenverkehr entdeckt

Netzwerkfreigabeaktivität deutet auf Datenverschlüsselung hin



MITRE ATT&CK in Flowmon ADS



Eingabedaten, Algorithmen und Ergebnisse

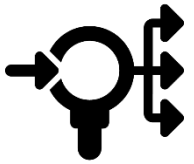
Eingabedaten

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

Algorithmen

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

Ergebnis

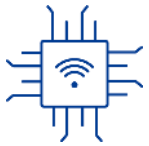


Ereignisse, relevante Telemetriedaten, forensische Erfassungsdaten und Analysen, Warnungen, Automatisierungen, CVE-Referenzen, frühere Vorfälle

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)