

# False Positives...

... are eating the SNOC

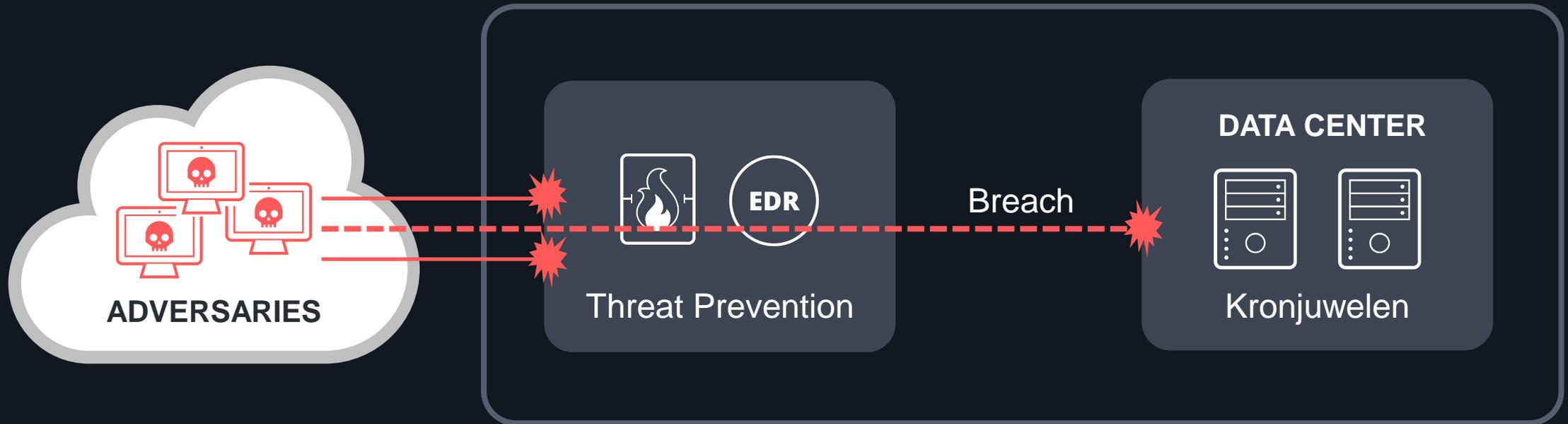
Jürgen Morgenstern, SE-Manager - DACH

NETSCOUT®

Guardians of the Connected World

# Status Quo - Cybersecurity

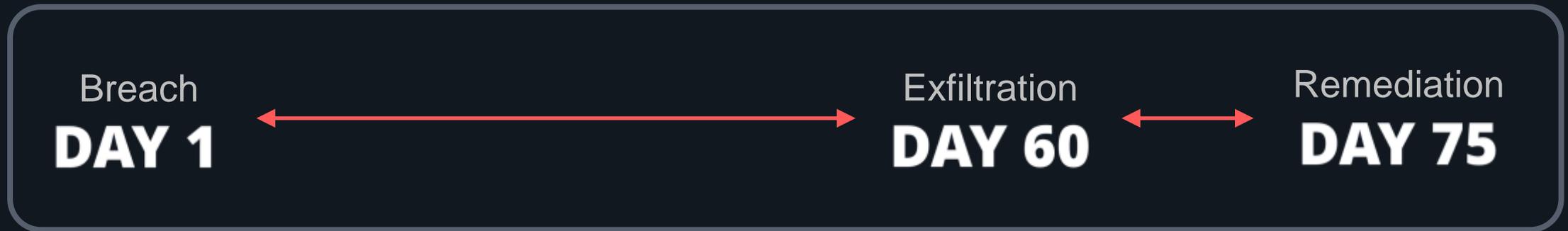
**Herausforderung:** Threat Prevention Tools können nicht alle Angriffe erkennen



**Immenses Investment und große Abhängigkeit von der Threat Prevention**  
**Die Situation im SOC hat sich nicht wesentlich verändert**  
**False Positives führen zu Alert Fatigue!**

# Status Quo - Cybersecurity

**Herausforderung:** Bei einer Kompromittierung bleiben Angreifer lange unentdeckt !



WARUM?

#1

Threat Prevention Tools sind für Day 1 konzipiert und erkennen die eigentliche Gefahr zu selten -> False Positives

#2

Threat Prevention Tools fehlt die Visibilität in die Bereiche, wo sich die Angriffe ausbreiten – Lack of evidence



# Status Quo - Cybersecurity

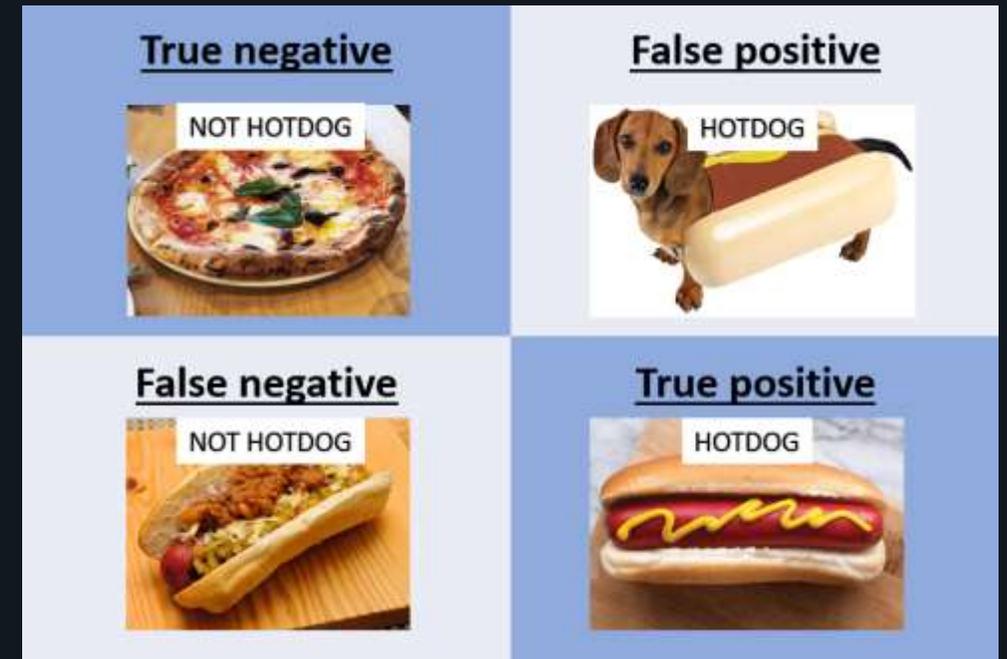
**Herausforderung:** Security Tools decken NICHT den kompletten Attack-Surface ab



Um Breaches zu erkennen, braucht es  
verlässliche Visibilität in alle Bereichen des Netzwerkes  
**VISIBILITÄT -> TRIAGE -> AKTION!**

# Status Quo - Resultat

1. Anzahl der Alarme ist zu hoch
  - >5k Events sind nicht handhabbar
2. Qualität der Alarme ist zu schlecht
  - zu wenig Context
  - zu abstrakt
3. Triage wird durch fehlende Informationen erschwert.



<https://blog.nillsf.com/index.php/2020/05/23/confusion-matrix-accuracy-recall-precision-false-positive-rate-and-f-scores-explained/>

-> ALERT FATIGUE



# Wie können/sollten wir mit FalsePositives umgehen?

# Netzwerkdaten helfen !!!

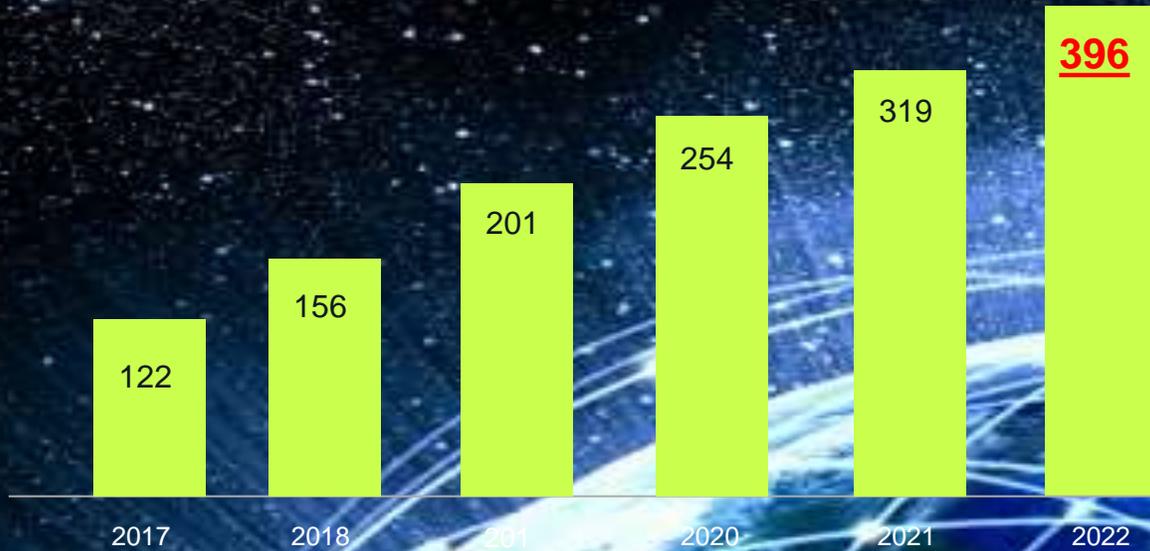


Cyber  
Triad

-  Data Center
-  Remote Sites
-  Cloud



# DATEN in BEWEGUNG



**Global IP Traffic**  
Exabytes/month

**26% CAGR**

Cisco VNI Global IP Traffic Forecast 2017-2022

**6 zettabytes**

Global consumer and business  
IP traffic will surpass **6**  
zettabytes per year by 2022.

zipdo



# Das Netzwerk bietet wichtige Informationen

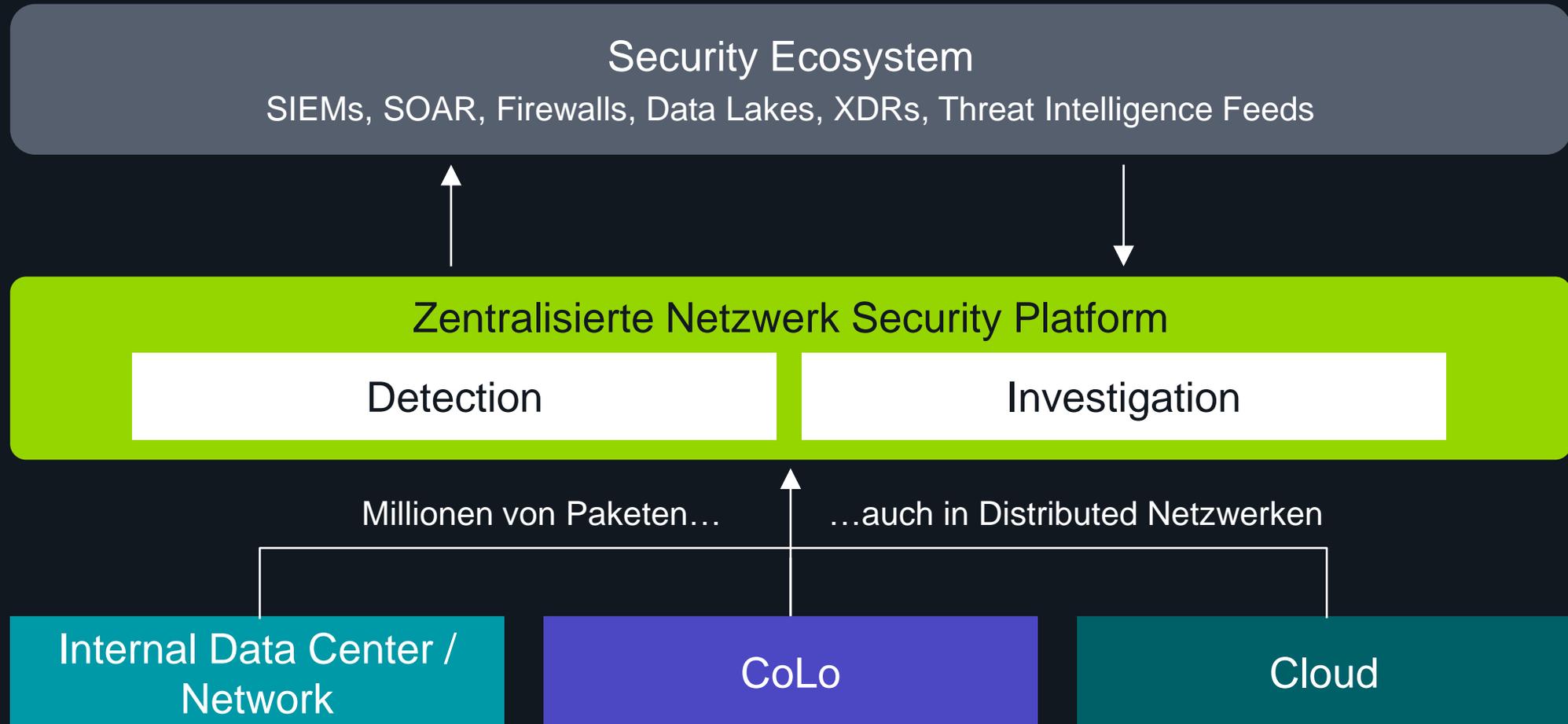
- Wer spricht mit wem? Wie oft?
- Was sind meine kritischen Assets, die ich schützen sollte?
- Wo sind diese Assets? (Public-cloud, remote, DC, etc.)
- Versucht jemand diese Assets zu discovern?
- Wie reagieren meine kritischen Assets darauf?
- Welche Daten werden ausgetauscht? Ist dabei etwas malicious?
- Wurden Daten exfiltriert? Falls ja, welche Daten?



**Pakete können diese und mehr Informationen beweiskräftig liefern!  
Alarme können einer schnellen Triage unterzogen werden!  
False Positives werden schnell erkannt!!!**



# Netscout Netzwerk Security Platform



# Evidence in Sekunden bei der Investigation

Reduzieren Sie die Mean Time to Restoration (MTTR)

Alert #	MTTR Facts #	MTTR Technique #	Asset/Rule #	Asset/Rule #	Asset/Rule #	Target #	Target Type #	Description #
1811-01-02 00:00:00	Information (11601)	Advanced Exp(11611)	Connection rule applied for domain query	18.200.101.10	18.200.101.10	18.200.101.10	IP_Address	18.200.101.10 is making more than 2000 DNS queries towards 192.168.10.100
1811-01-02 00:00:00	Information (11601)	Advanced Exp(11611)	Connection rule applied for domain query	18.200.101.10	18.200.101.10	18.200.101.10	IP_Address	18.200.101.10 is making more than 2000 DNS queries towards 192.168.10.100
1811-01-02 00:00:00	Domain and Internal (11601)	Advanced Exp(11611)	Connection rule applied for domain query	18.200.101.10	18.200.101.10	18.200.101.10	IP_Address	18.200.101.10 is making more than 2000 DNS queries towards 192.168.10.100
1811-01-02 00:00:00	Domain and Internal (11601)	Advanced Exp(11611)	Connection rule applied for domain query	18.200.101.10	18.200.101.10	18.200.101.10	IP_Address	18.200.101.10 is making more than 2000 DNS queries towards 192.168.10.100

Alert  
└─▶



Who...?  
When...?  
What...?  
How...?

└─▶

MS Name	Application	Server Name	Server Port	Client Name	Identity	Avg RT (ms)	App Errors	Retries	Timeouts	Aggr.UL	Start time	Duration	Status
DC01-Internet	SMTP	peoplemanagement.co...	443	10.30.15.5	-	7.40	0	0	0	0	5/26/2023 4:47:30 PM	00:00:00.245	OK
DC02-Internet	SMTP	peoplemanagement.co...	443	10.30.15.6	-	0.65	0	0	0	0	5/26/2023 4:47:30 PM	00:00:00.289	OK
DC03-Internet	SMTP	peoplemanagement.co...	443	10.30.15.8	-	4.50	0	0	0	0	5/26/2023 4:47:30 PM	00:00:14.883	OK
DC04-Internet	SMTP	peoplemanagement.co...	443	10.30.15.8	-	0.81	0	0	0	0	5/26/2023 4:48:02 PM	00:00:00.371	OK
DC05-Internet	SMTP	peoplemanagement.co...	443	10.30.15.5	-	0.89	0	0	0	0	5/26/2023 4:48:02 PM	00:00:00.311	OK

Description	Relative Time	10.30.15.5	192.168.10.100	10.30.15.5
TCP Connection Start	00:00:00.000000			
TCP Connection End	00:00:00.245072			

Entity	Value	Interface	DC01-Internet
Start time	5/26/2023 4:47:30 PM	Client IP - Port	10.30.15.5:443
End time	5/26/2023 4:47:30 PM	Client to Server Bytes	14.8 K
Client IP Address	10.30.15.5	Client to Server Packets	40
Server IP Address	192.168.10.1	Server to Client Bytes	19.1 K
Total Connections	1	Server to Client Packets	37



# Reaktives vs. Proaktives Threat Hunting

Reaktiv und zeitraubend



Proaktiv and effizient → führt zu einem besseren Security Posture



# Vielen DANK !!!

[Juergen.Morgenstern@netscout.com](mailto:Juergen.Morgenstern@netscout.com)



NETSCOUT®

Guardians of the Connected World