NETSCOUT

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 Anfriffe erkennen

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

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

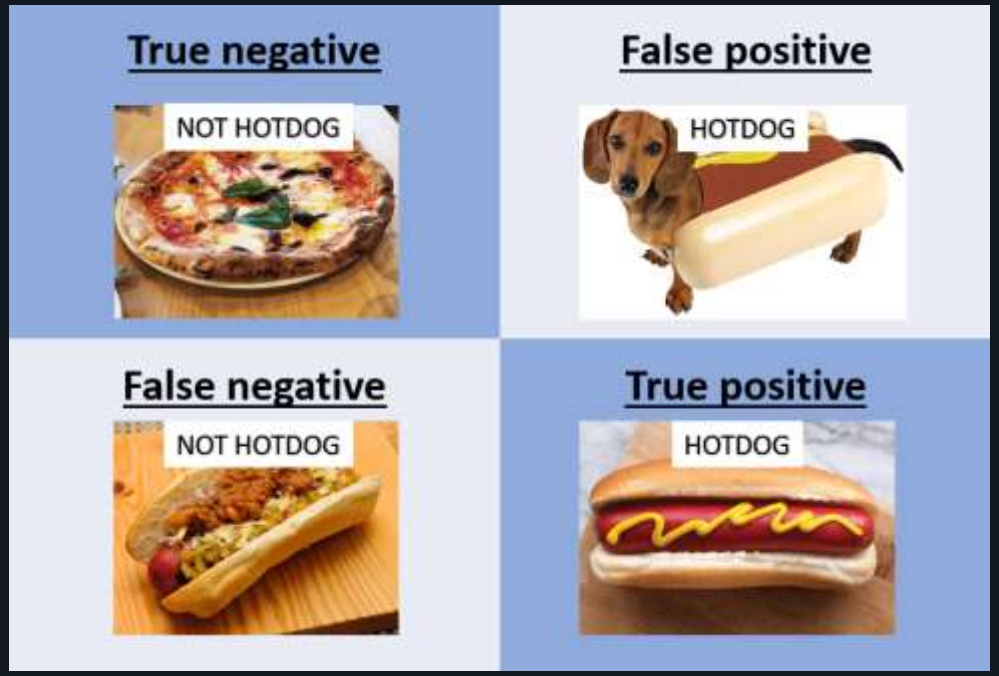
Herausforderung: Security Tools decken NICHT den kompletten Attack-Surface ab

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.

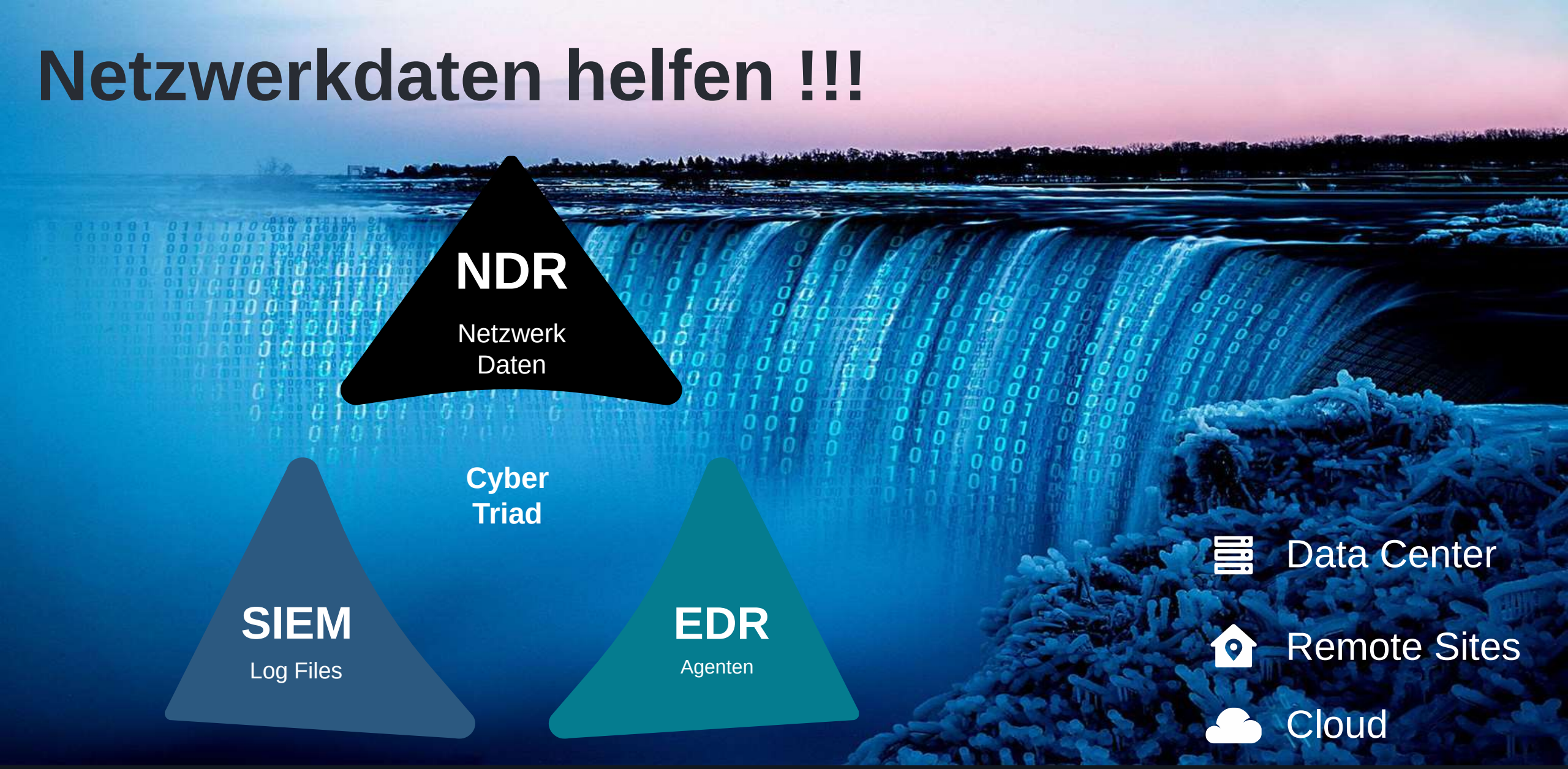
-> ALERT FATIQUE



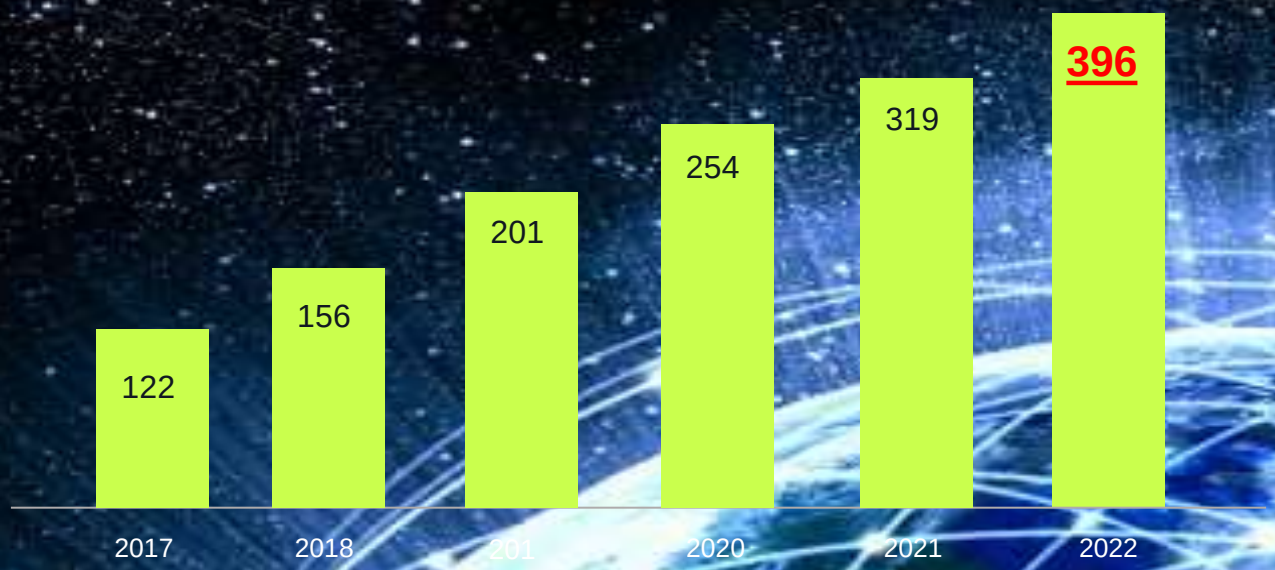
https://blog.nillsf.com/index.php/2020/05/23/confusion-matrix-accuracy-recall-precision-false-positive-rate-and-f-scores-explained/

Wie können/sollten wir mit FalsePositives umgehen?

Netzwerkdaten helfen !!!



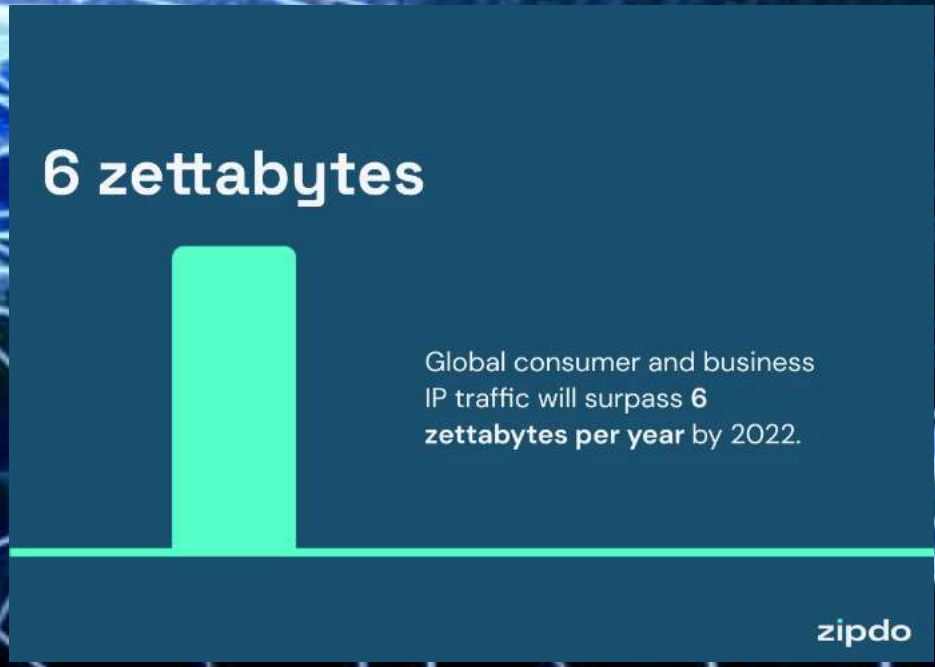
DATEN in BEWEGUNG



Global IP Traffic
Exabytes/month

26% CAGR

Cisco VNI Global IP Traffic Forecast 2017-2022

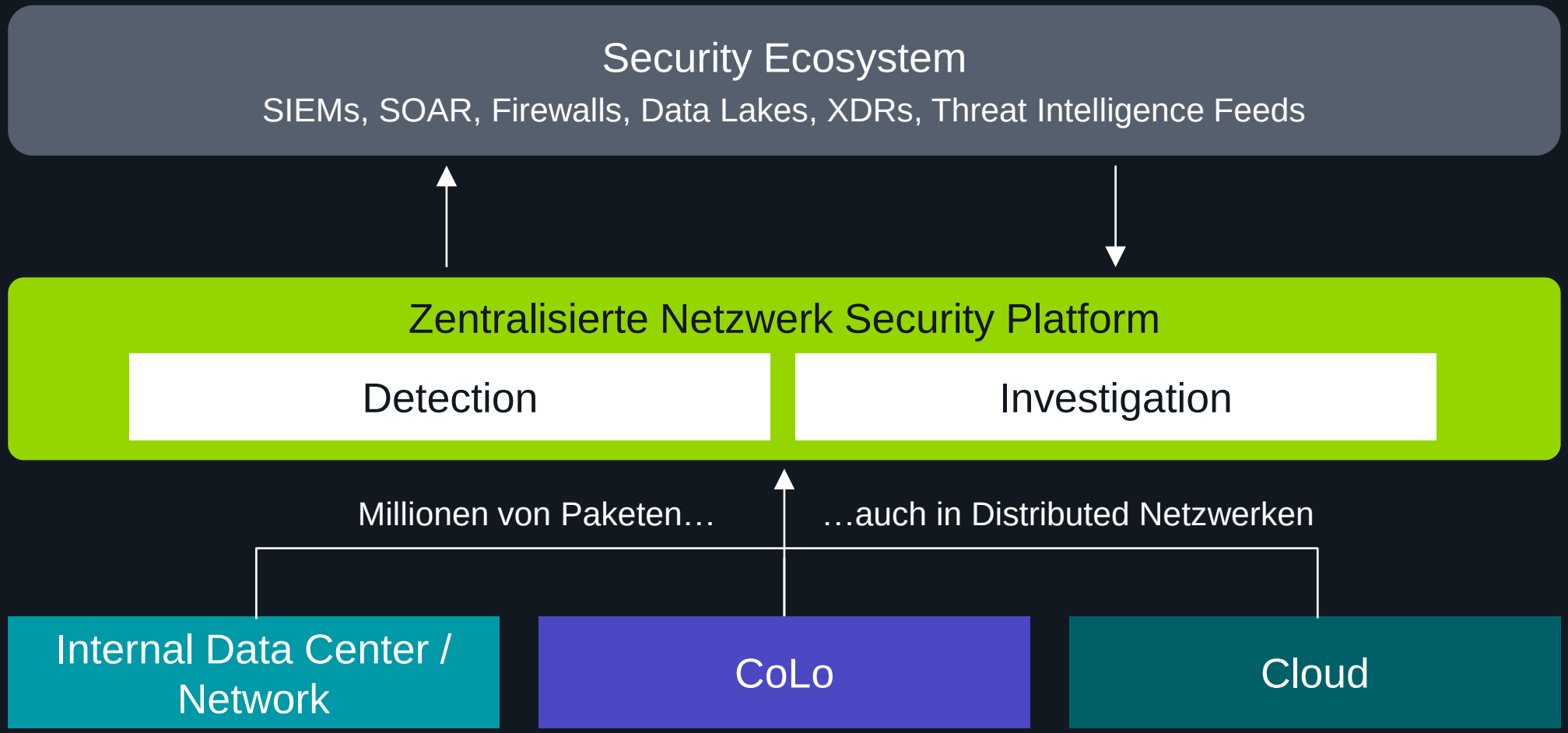


Das Netzwerk bietet wichtige Informationen

- 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 warden ausgetauscht? Ist dabei etwas malicious?
- Wurden Daten exfiltriert? Fals ja, welche Daten?

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

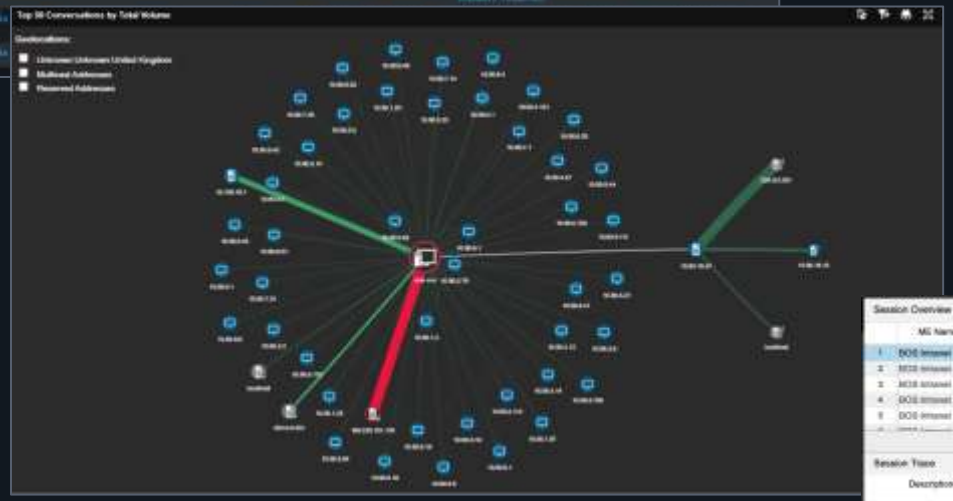
Netscout Netzwerk Security Platform



Evidence in Sekunden bei der Investigation

Reduzieren Sie die Mean Time to Restoration (MTTR)

Alert

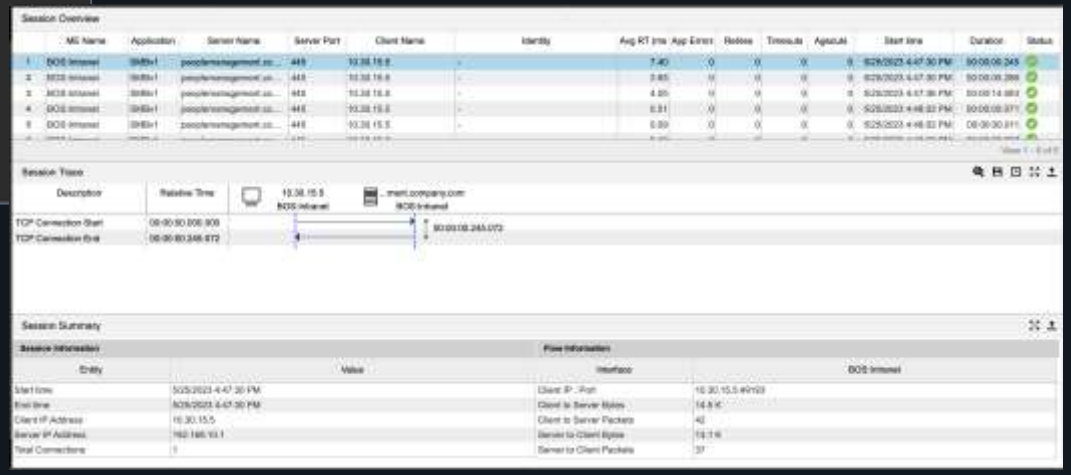


Who…?

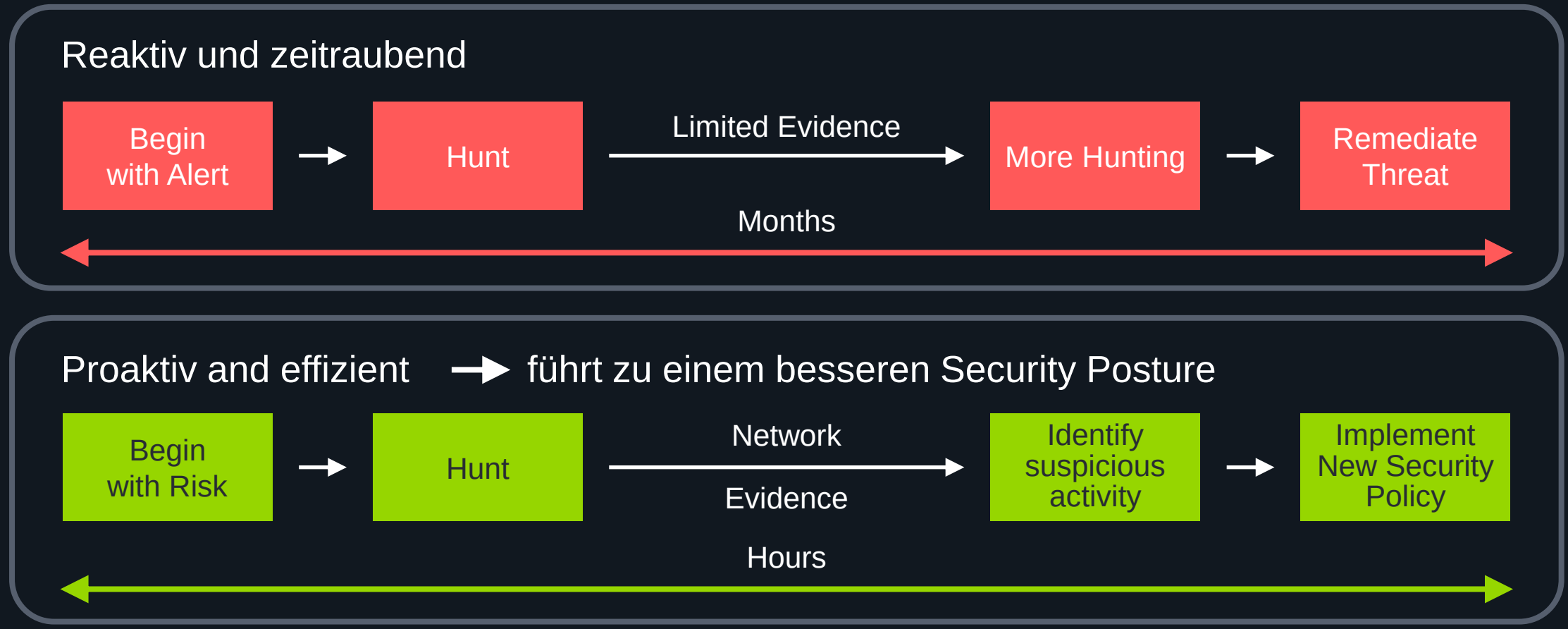
When… ?

What… ?

How… ?



Reaktives vs. Proaktives Threat Hunting



Vielen DANK !!!

Juergen.Morgenstern@netscout.com

NETSCOUT®

Guardians of the Connected World