Automatisierung macht uns das Leben leichter.

Automatisierung hilft uns, schneller bessere Entscheidungen zu treffen.

Automatisierung ist toll.

Wir alle lieben Automatisierung.

Außer wenn wir es nicht tun.

Log-Normalisierung

für skalierbare Datenanreicherung von SIEM-Use-Cases

8COM
CYBER SECURITY

Log-Normalisierung

für skalierbare Datenanreicherung von SIEM-Use-Cases

8COM CYBER SECURITY

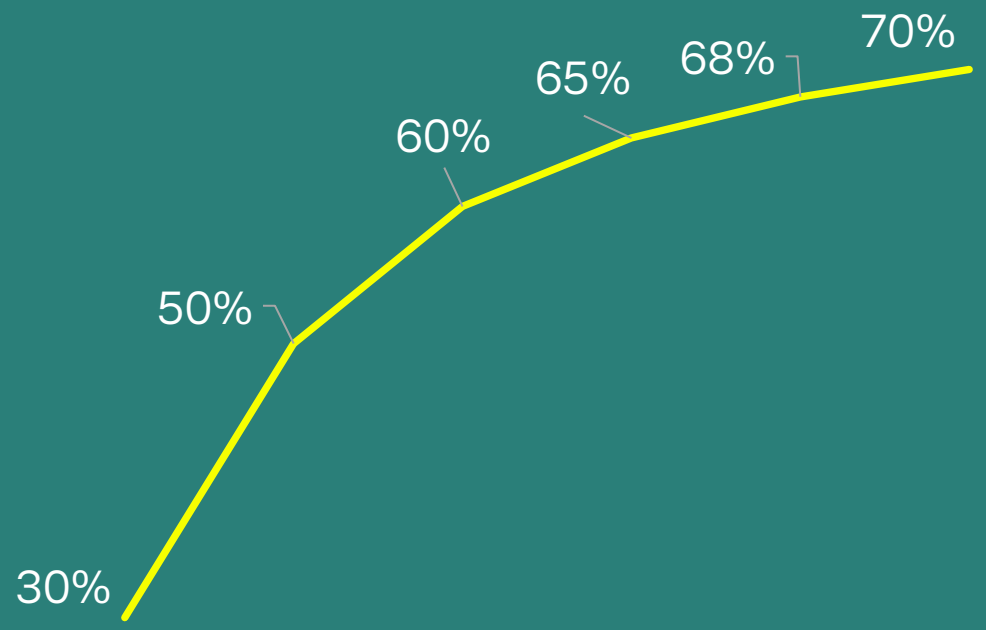
Die Herausforderung

Skalierbare
Datenanreicherung von SIEM-Use-Cases

Automatisierung hat diminishing returns...

...aber über all unsere Kunden gerechnet bringen selbst aufwändige Automatisierungen schnell einen Benefit

8COM CYBER SECURITY



Use Cases

Abuse of BITS Client

- Microsoft-Windows-Bits-Client
- Event IDs: 59, 60, 61
  - Zeitpunkt
  - System, auf dem Job angelegt wurde
  - Ziel-URL
  - Benutzer, der Job angelegt hat

User Account was Created with a Dollarsign

1. Eventlog: Security
2. Event ID: 4720
   a. Zeitpunkt
   b. System, auf dem der Benutzer angelegt wurde
   c. Quellkonto
   d. Neues Konto


WHOOSH YOU AUTOMATED NOW

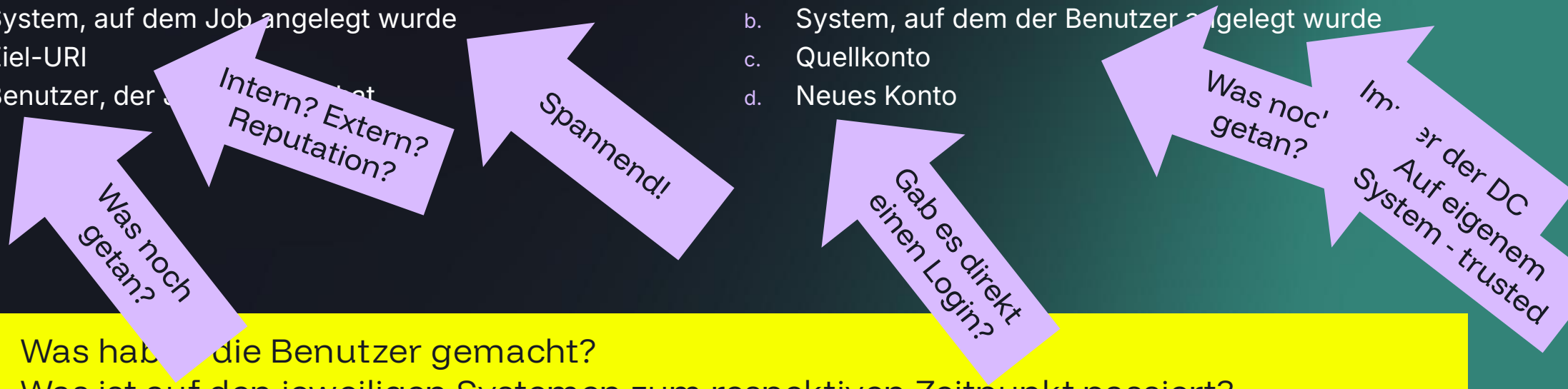
Headline 1

Abuse of BITS Client

- Microsoft-Windows-Bits-Client
- Event IDs: 59, 60, 61
  - Zeitpunkt
  - System, auf dem Job angelegt wurde
  - Ziel-URI
  - Benutzer, der

User Account was Created with a Dollarsign

1. Eventlog: Security
2. Event ID: 4720
   a. Zeitpunkt
   b. System, auf dem der Benutzer angelegt wurde
   c. Quellkonto
   d. Neues Konto

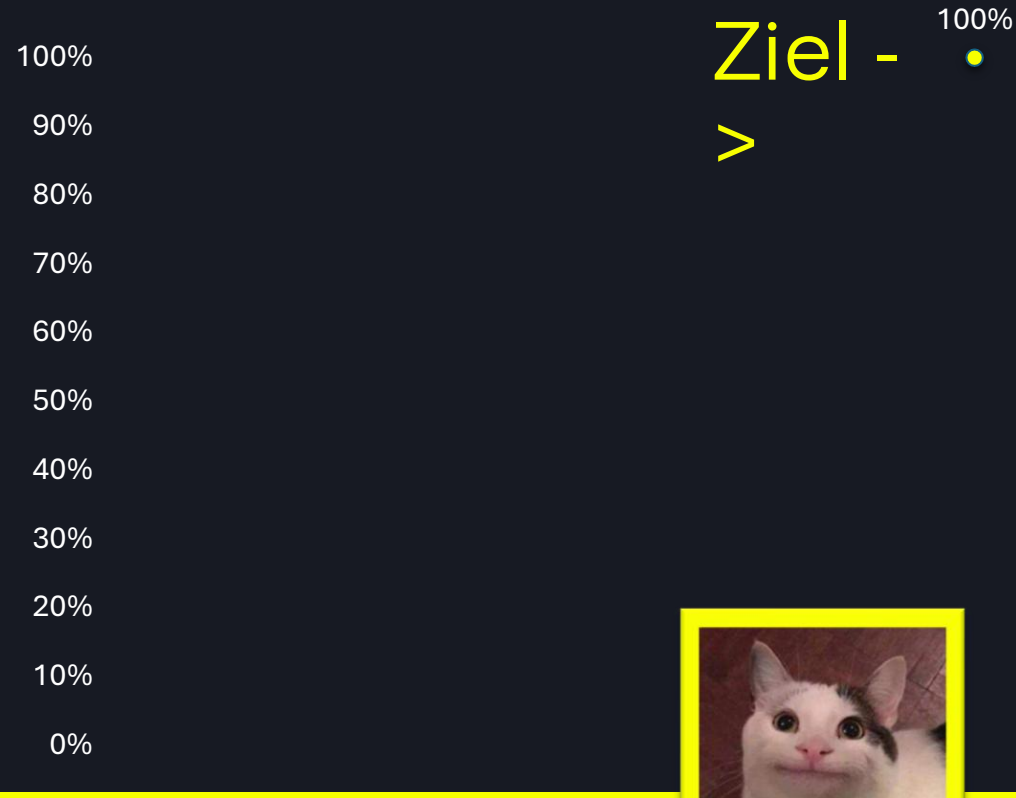


Was haben die Benutzer gemacht?
Was ist auf den jeweiligen Systemen zum respektiven Zeitpunkt passiert?

Zwischenbericht!

Was haben wir erreicht?

3 Use Cases automatisiert!



Sehr unterschiedliche Analyse je nach Use Case nötig
…bei hunderten an Use Cases keine Einzelbehandlung möglich

8COM

Option 3

Relevante Daten klassifizieren und die Use Cases selbst anpassen

💗 Alles an einer Stelle, ein einheitliches Runbook

Normalisierung ist sinnvoll, aber…

8COM

Abuse of BITS Client

- Zeitpunkt
- System, auf dem Job angelegt wurde (“host”)
- Ziel-URI (“uri”)
- Benutzer, der Job angelegt hat (“user”)

User Account was Created with a Dollarsign

1. Zeitpunkt
2. System, auf dem der Benutzer angelegt wurde (“host”)
3. Quellkonto („user“)
4. Neues Konto („target_user“)

DDOS Attack

- Zeitpunkt
- Erkennendes System (“host”)
- Quelladressen (“sources”)
- Zieladresse (“target”)
- Ziel-URI (“uri”)

…nicht immer zielführend
Oft werden aber Dinge, die wenig miteinander zu tun haben, unter einen Hut gepackt.


I'LL CREATE MY OWN NORMALIZATION
WITH BLACKJACK AND HOOKERS

Normalisierung ist sinnvoll, aber…

8COM

Abuse of BITS Client

- Zeitpunkt
- suspicious_host
- suspicious_uri
- suspicious_user

User Account was Created with a Dollarsign

1. Zeitpunkt
2. System, auf dem der Benutzer angelegt wurde (“host”)
3. admin_user
4. suspicious_user

DDOS Attack

- Zeitpunkt
- internal_host
- external_host (Liste)
- Zieladresse (“target”)
- internal_uri

suspicious_us

- Auffälligkeit bei Anmeldung?
- Andere Prozesse?
- …

admin_user

- Auffälligkeit bei Anmeldung?
- Dienstzeit?
- …

cloud_user

- 2FA aktiv?

suspicious_uri

- Reputation?
- …

internal_uri

Nix!

…

…

…

…

…

…

8COM CYBER SECURITY

Zwischenbericht!

Was haben wir erreicht?

Zahlreiche Use Cases automatisiert!

„nur mal fix“ sprechende Namen vergeben

Pain Points

Lernen trotz Schmerzen

1. Jeder Use Case muss betrachtet und dessen Daten klassifiziert werden
2. Strikt daran halten, Daten als das zu benennen, was sie repräsentieren
3. Automatisierungen bauen, die für passende Daten ausgeführt werden

8COM

Sie haben noch Fragen?

Sprechen Sie mich gerne an!

8COM
CYBER SECURITY

Dominik Schmidt
Teamlead SIEM

dominik.schmidt@8com.de
www.8com.de

8com.de/newsletter