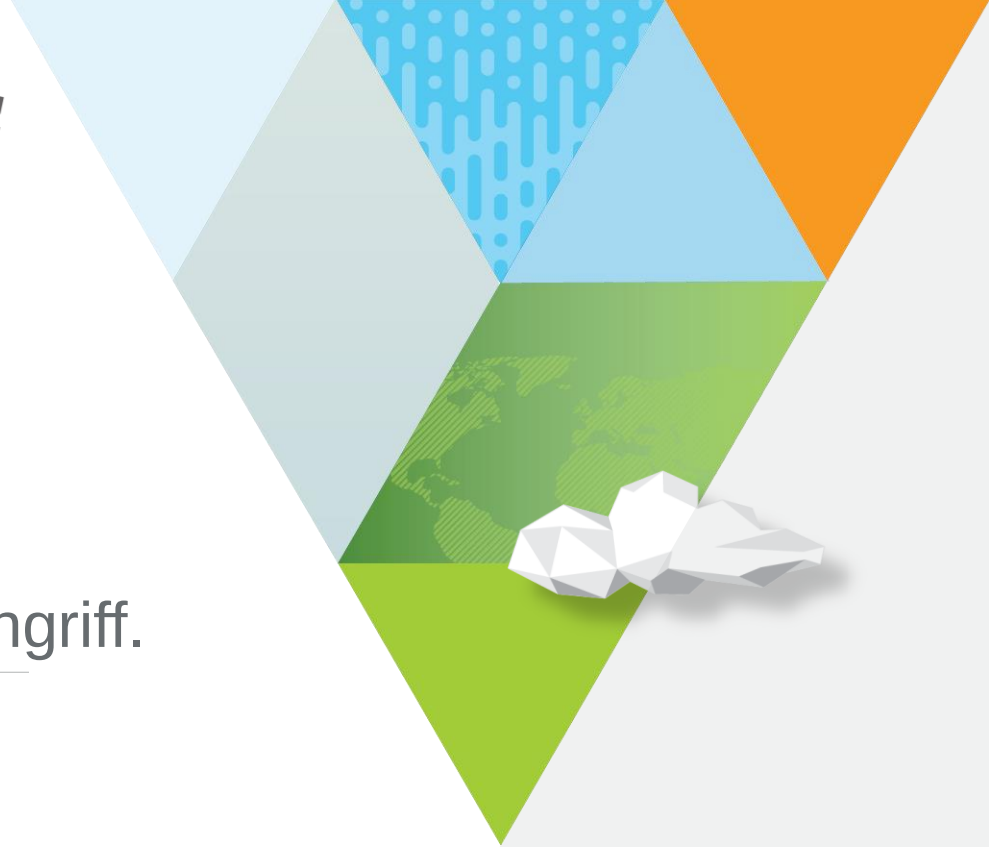
VECTRA
SECURITY THAT THINKS.®

EDAG



Erfahrungen aus dem Cyberangriff.

MBUF IT Security Spotlight Day
18.11.2021

Moderation

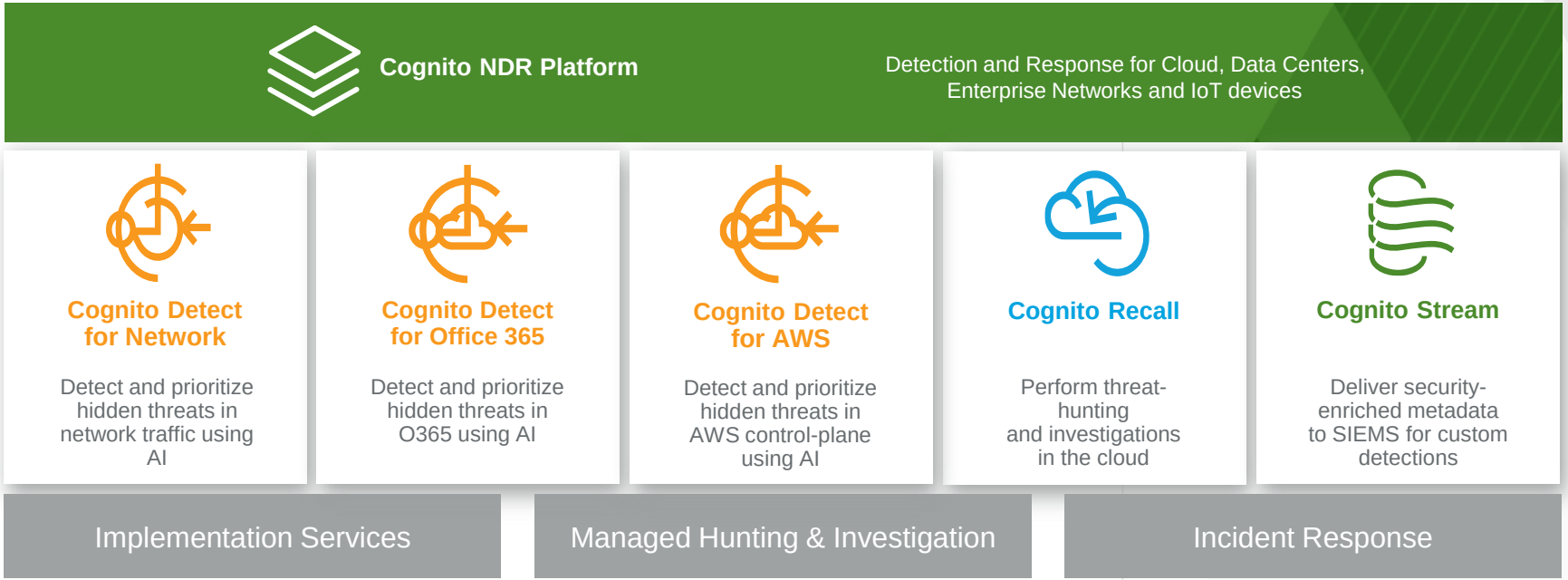
Maria Fladung

EDAG Group

Matthias Schmauch

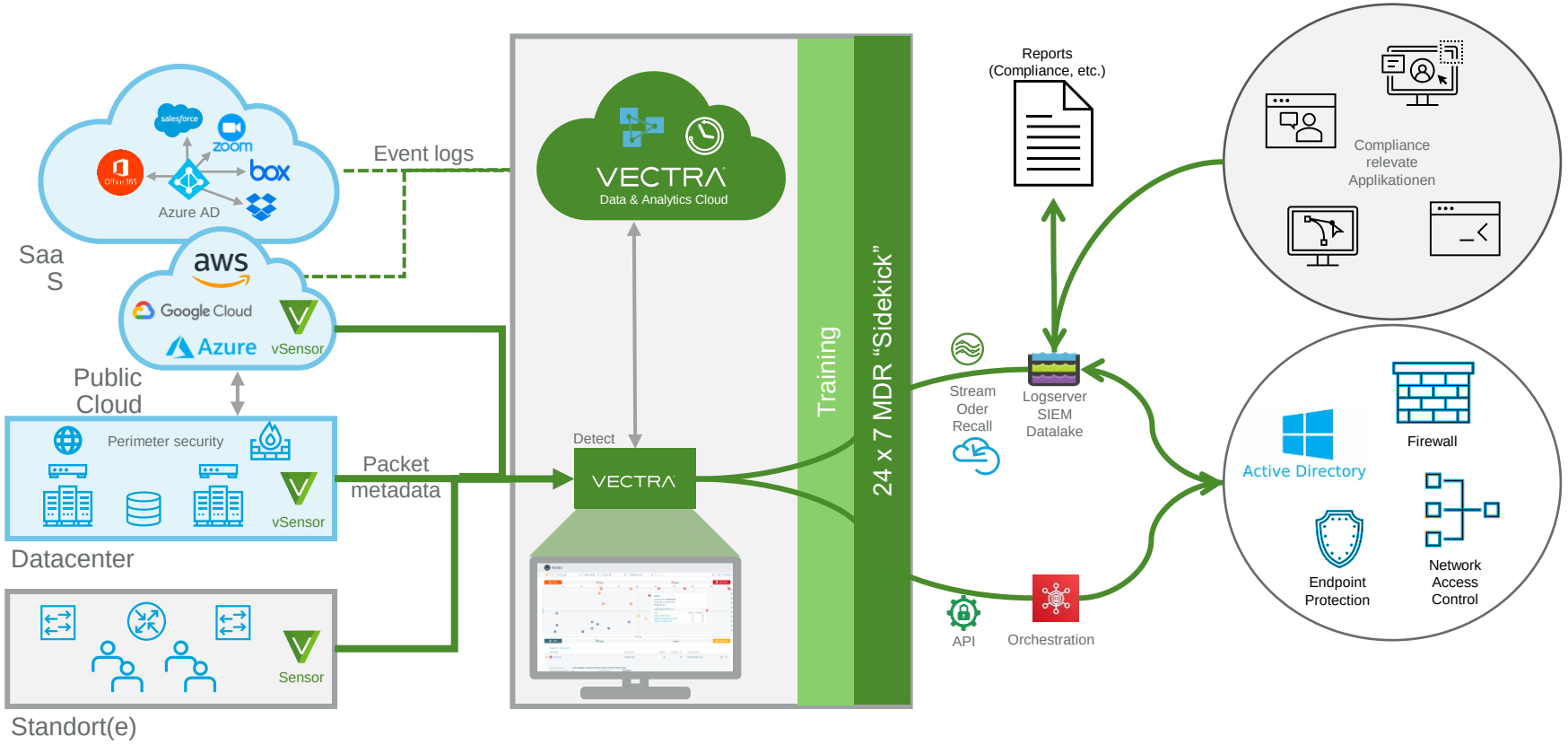
Vectra AI

Cognito Network Detection & Response Platform



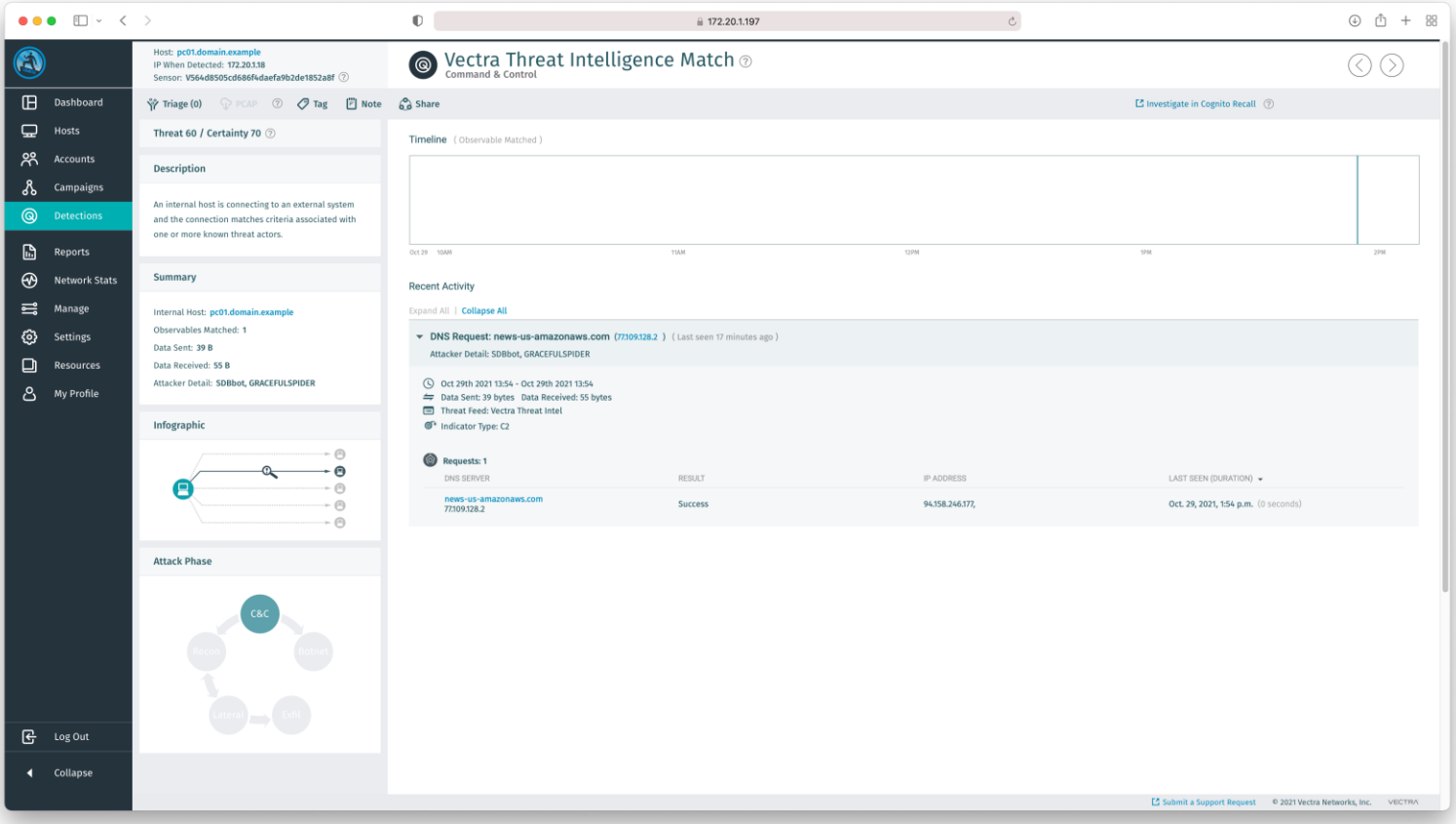
Die Cognito-Plattform sammelt und analysiert Netzwerk-Metadaten und reichert sie mit maschinellem Lernen an

Architektur: Angriffserkennung für Netzwerk und Cloud

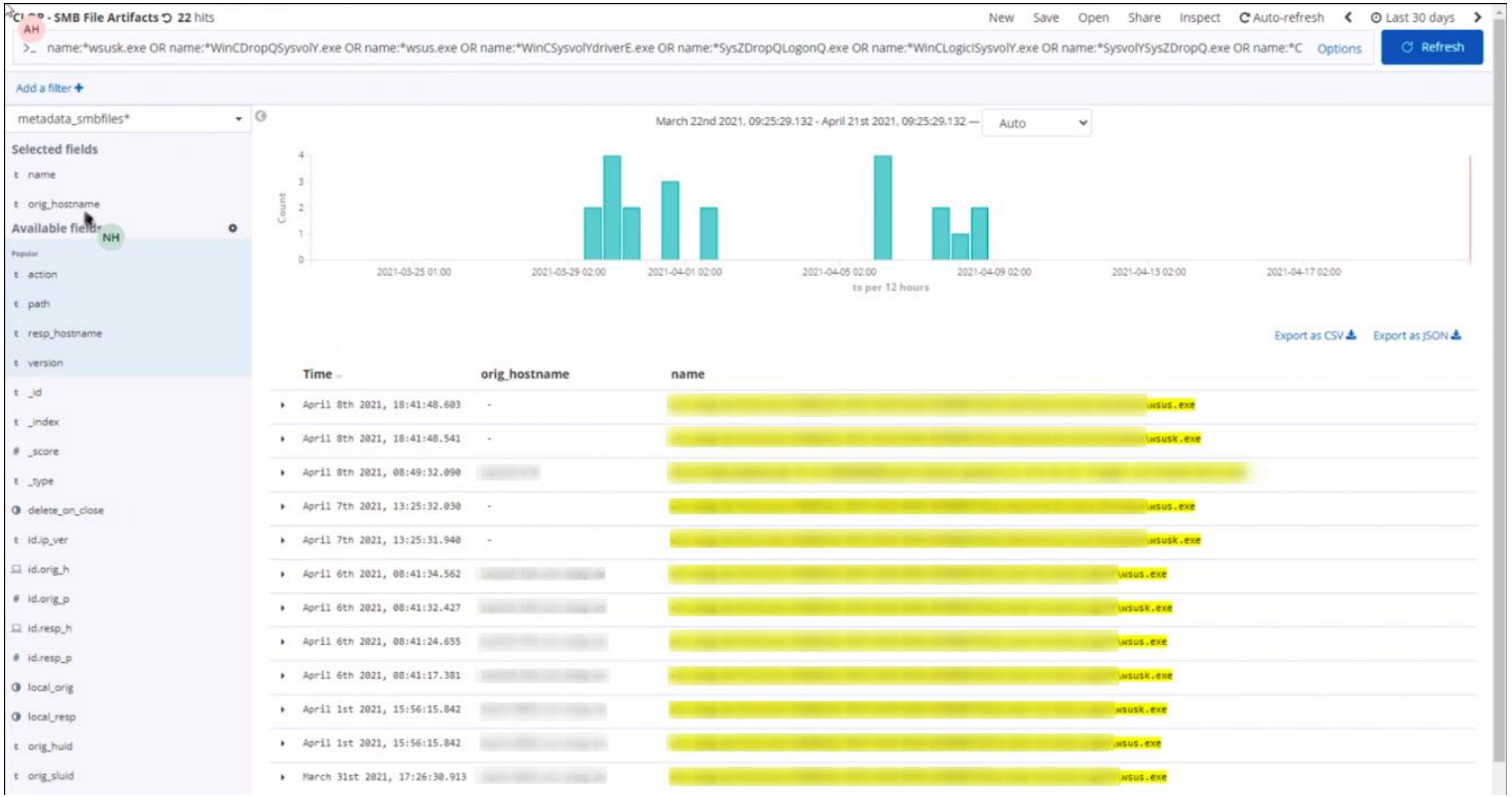


VECTRA
SECURITY THAT THINKS®

Threat Intelligence Match



IOC hunting


CL_R - SMB File Artifacts 22 hits
New Save Open Share Inspect Auto-refresh Last 30 days
name:*wsusk.exe OR name:*WinCDropQSysvolY.exe OR name:*wsus.exe OR name:*WinCSysvolYdriverE.exe OR name:*SysZDropQLogonQ.exe OR name:*WinCLogicISysvolY.exe OR name:*SysvolYSysZDropQ.exe OR name:*C
Options
Refresh
Add a filter
metadata_smbfiles*
Selected fields
t name
t orig_hostname
Available fields
Popular
t action
t path
t resp_hostname
t version
t _id
t _index
_score
t _type
delete_on_close
t id.ip_ver
id.orig_h
id.orig_p
id.resp_h
id.resp_p
local_orig
local_resp
t orig_huid
t orig_sluid
March 22nd 2021, 09:25:29.132 - April 21st 2021, 09:25:29.132 —
Auto
Count
2021-03-25 01:00
2021-03-29 02:00
2021-04-01 02:00
2021-04-05 02:00
2021-04-09 02:00
2021-04-13 02:00
2021-04-17 02:00
ts per 12 hours
Export as CSV
Export as JSON
Time
orig_hostname
name
April 8th 2021, 18:41:48.603
April 8th 2021, 18:41:48.541
April 8th 2021, 08:49:32.090
April 7th 2021, 13:25:32.030
April 7th 2021, 13:25:31.940
April 6th 2021, 08:41:34.562
April 6th 2021, 08:41:32.427
April 6th 2021, 08:41:24.655
April 6th 2021, 08:41:17.381
April 1st 2021, 15:56:15.842
April 1st 2021, 15:56:15.842
March 31st 2021, 17:26:30.913

Fragen & Antworten

Mehr erfahren

IDC: Business Value of Cognito NDR

Case Study: EDAG

Case Study: Rossmann

Case Study: Fenaco

Danke