

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



Cognito NDR Platform

Detection and Response for Cloud, Data Centers,
Enterprise Networks and IoT devices



Cognito Detect for Network

Detect and prioritize
hidden threats in
network traffic using
AI



Cognito Detect for Office 365

Detect and prioritize
hidden threats in
O365 using AI



Cognito Detect for AWS

Detect and prioritize
hidden threats in
AWS control-plane
using AI



Cognito Recall

Perform threat-
hunting
and investigations
in the cloud



Cognito Stream

Deliver security-
enriched metadata
to SIEMS for custom
detections

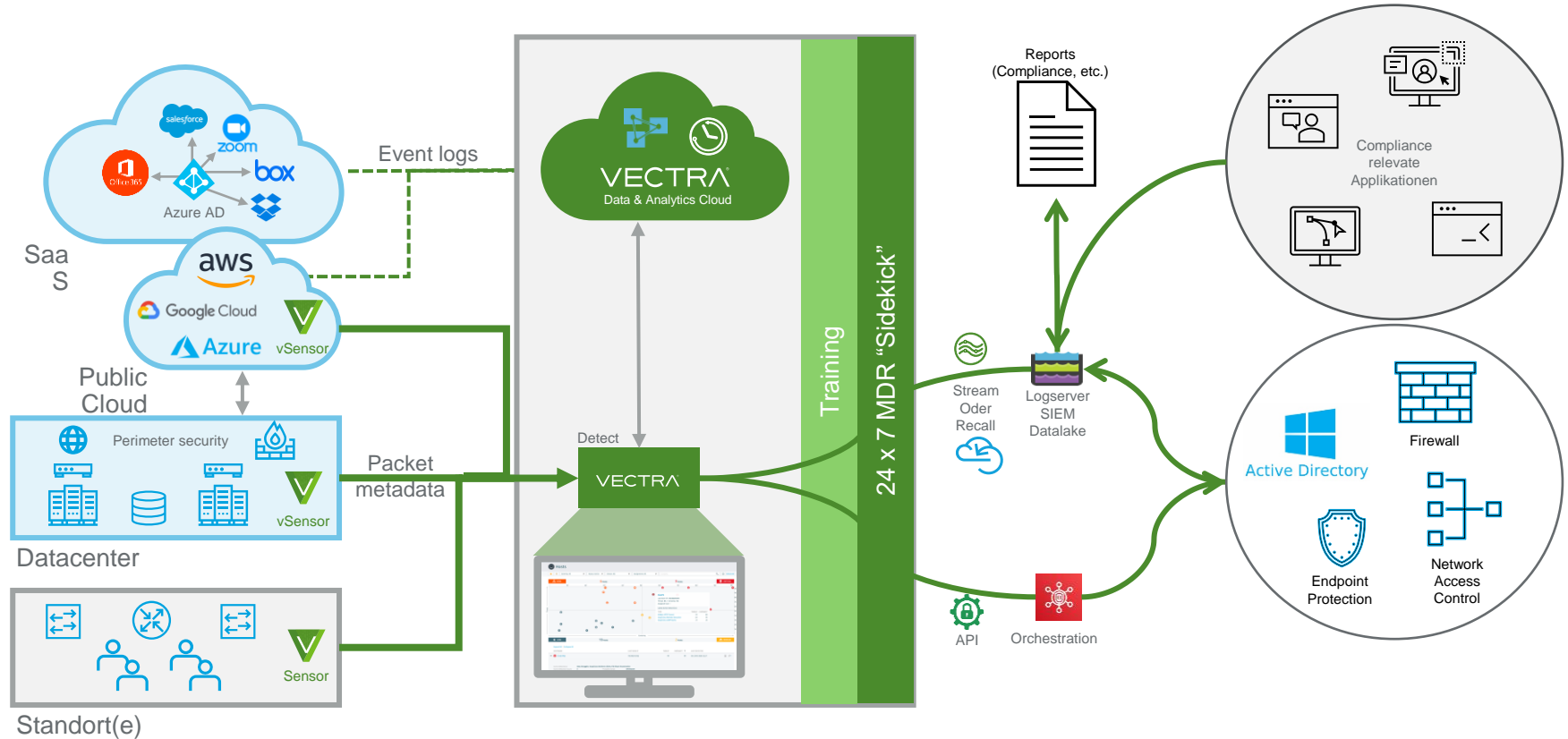
Implementation Services

Managed Hunting & Investigation

Incident Response

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

Architektur: Angriffserkennung für Netzwerk und Cloud

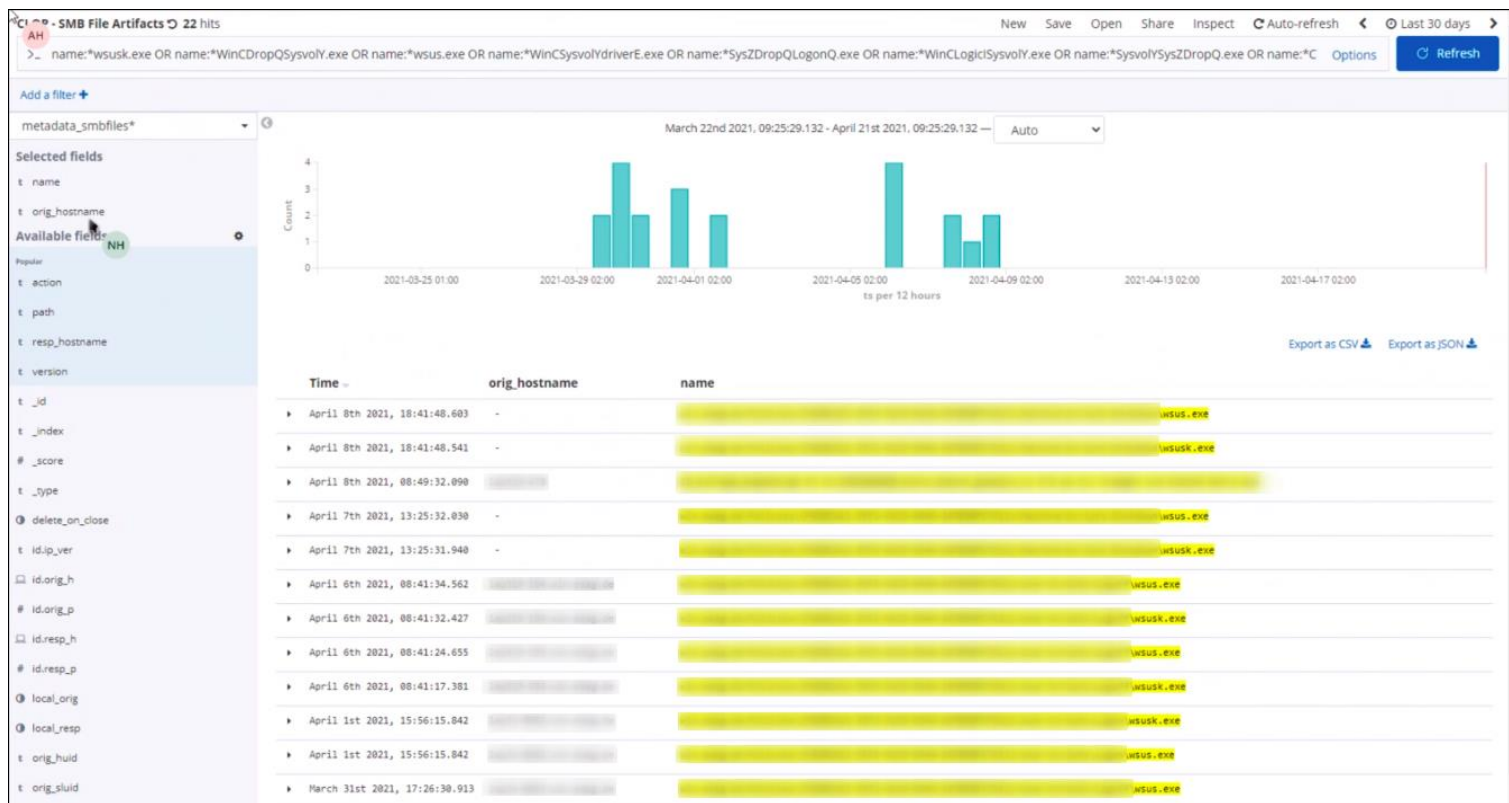


Threat Intelligence Match

The screenshot displays the Vectra Threat Intelligence Match interface. The left sidebar contains navigation options: Dashboard, Hosts, Accounts, Campaigns, **Detections**, Reports, Network Stats, Manage, Settings, Resources, and My Profile. The main content area is titled "Threat 60 / Certainty 70" and includes sections for Description, Summary, Infographic, and Attack Phase. The Description states: "An internal host is connecting to an external system and the connection matches criteria associated with one or more known threat actors." The Summary section shows: "Internal Host: pc01.domain.example", "Observables Matched: 1", "Data Sent: 39 B", "Data Received: 55 B", and "Attacker Detail: SDBot, GRACEFULSPIDER". The Infographic shows a host icon connected to several external system icons. The Attack Phase diagram shows a cycle: C&C -> Recon -> Lateral -> Exfil -> Botnet -> C&C. The right pane shows a "Timeline (Observable Matched)" which is currently empty. Below the timeline is the "Recent Activity" section, which is expanded to show a "DNS Request: news-us-amazonaws.com (77109128.2)" detected 17 minutes ago. The attacker detail is "SDBot, GRACEFULSPIDER". The activity log shows a request from Oct 29th 2021 13:54 to Oct 29th 2021 13:54, with 39 bytes sent and 55 bytes received. The threat feed is "Vectra Threat Intel" and the indicator type is "C2". Below this is a table of requests:

Requests: 1	RESULT	IP ADDRESS	LAST SEEN (DURATION)
DNS SERVER news-us-amazonaws.com 77109128.2	Success	94.158.246.177	Oct 29, 2021, 1:54 p.m. (0 seconds)

IOC hunting



Fragen & Antworten



Mehr erfahren

An IDC Business Value White Paper, sponsored by Vectra



The Business Value of Cognito Network Detection and Response from Vectra

RESEARCH BY:

- Christopher Kinsel**
Research Director
Security & Trust Products, IDC
- Matthew Marston**
Research Director
Business Value Strategy Practice, IDC

IDC: Business Value of Cognito NDR

Orange Cyberdefense

Kundenreferenz

EDAG setzt nach Ransomware-Angriffe auf Vectra - KI-basierte Cyberabwehr sichert Neustart und Betrieb des Netzwerks



With more than 2,256 employees in Germany and another 1,492 stores in Eastern and Southeastern Europe, ROSSMANN is one of the largest retail chains in Europe, with a total of 4,086 stores and 56,200 employees. As one of the largest retailers in Germany, ROSSMANN IT security team needed assistance to quickly restore access to network.

The ROSSMANN IT security team, headed by Tom Land (see below), faced the prospect of ransomware in its security center to which cybercriminals, at its own expense, were to attempt to restore the network.

After evaluating solutions in the area of console-based intrusion prevention, ROSSMANN considered what had worked to identify potential security misconfigurations and vulnerabilities.

The results of this evaluation had been used through analysis of the SOC phase. The team ultimately chose a diverse number of solutions that included the Vectra Threat Containment Index™ (VTCI) solution for ransomware.

"The Vectra Threat Containment Index™ automatically prioritizes detections and its ability to see the most critical threat behaviors. For us, it coordinates hundreds of experts and technical contacts to prevent root devices that pose the biggest threat."

Tom Land
Security Team Lead
ROSSMANN IT

Case Study: EDAG

VECTRA

Case Study

Vectra stops data breaches across one of Europe's largest drug store chains



Organization: ROSSMANN
Industry: Retail
Country: Germany

Challenge

Ransomware to quickly threat behavior and disruption without loss of critical data

Solution criteria

- Customers to describe an incident and plan that requires immediate response to identify those who are going to be affected by the breach
- Incident response to be completed as early as possible
- Automated response with integration to the threat intelligence

David Lehmann
Security Team Lead
ROSSMANN IT

Case Study: Rossmann

VECTRA

Case Study

Mega-producer of consumer goods relies on Vectra in the SOC



Organization: fenaco
Industry: Retail
Country: Switzerland

Challenge

Identifying security incidents and threat intelligence to prevent security breaches

Solution criteria

- To detect security incidents and respond quickly to security incidents
- To detect security incidents and respond quickly to security incidents

Stefan Wenz
Security Operations Manager
fenaco AG

Case Study: Fenaco



Danke



VECTRA[®]
SECURITY THAT THINKS.[®]