



Chancen der Gefahrenerkennung mit einem SIEM System

Sarah Piotrowski, Jens Hektor
IT Center der RWTH Aachen University
80. DFN Betriebstagung, 20.03.2024

Agenda

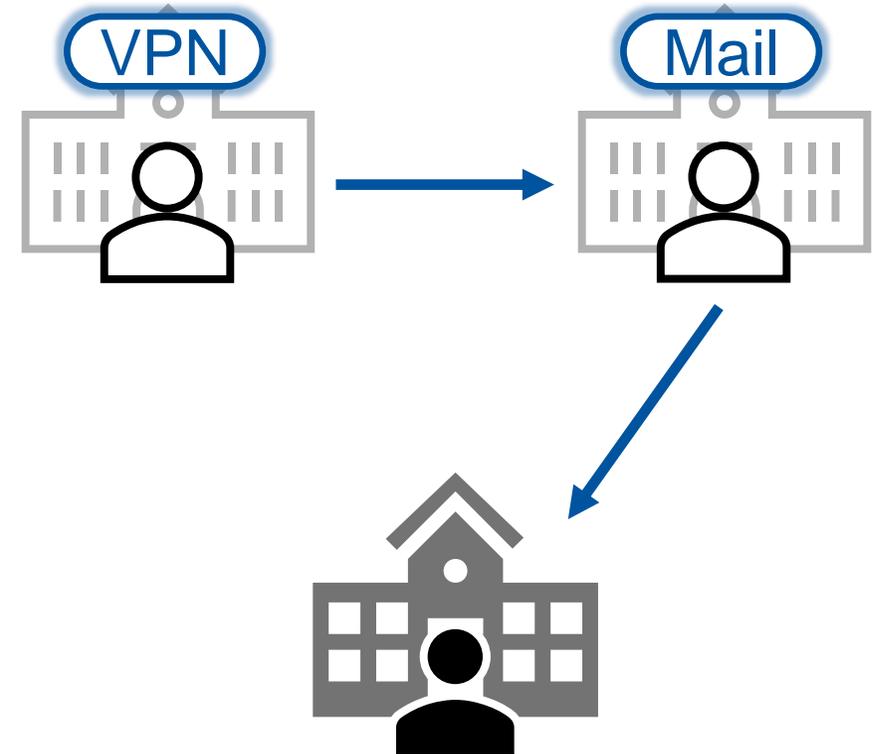
- Aktuelle Situation
- Beschaffung
- ELK Stack
- Beispiele mit Exchange Daten
- Enrichment

Situation

- Geleakter VPN Account Uni A
- Geleakter E-Mail Account Uni B
- Opfer Uni C empfängt E-Mail von B, initiiert von A

- Antworten auf geleakte E-Mails eines Users an die Kollegen

- Hinweise von Extern auf geleakte Accounts



Handlungsbedarf

- VPN goes MFA
- E-Mail ist da sperriger

- Analyse Logfiles:
Radius, Active Directory
Netflow, Firewall, NAT
Serverlogs, SSO, speziell Exchange
- Identitäten:
RWTH-Kennung
WLAN-Kennung
interne Exchange-Kennung
...

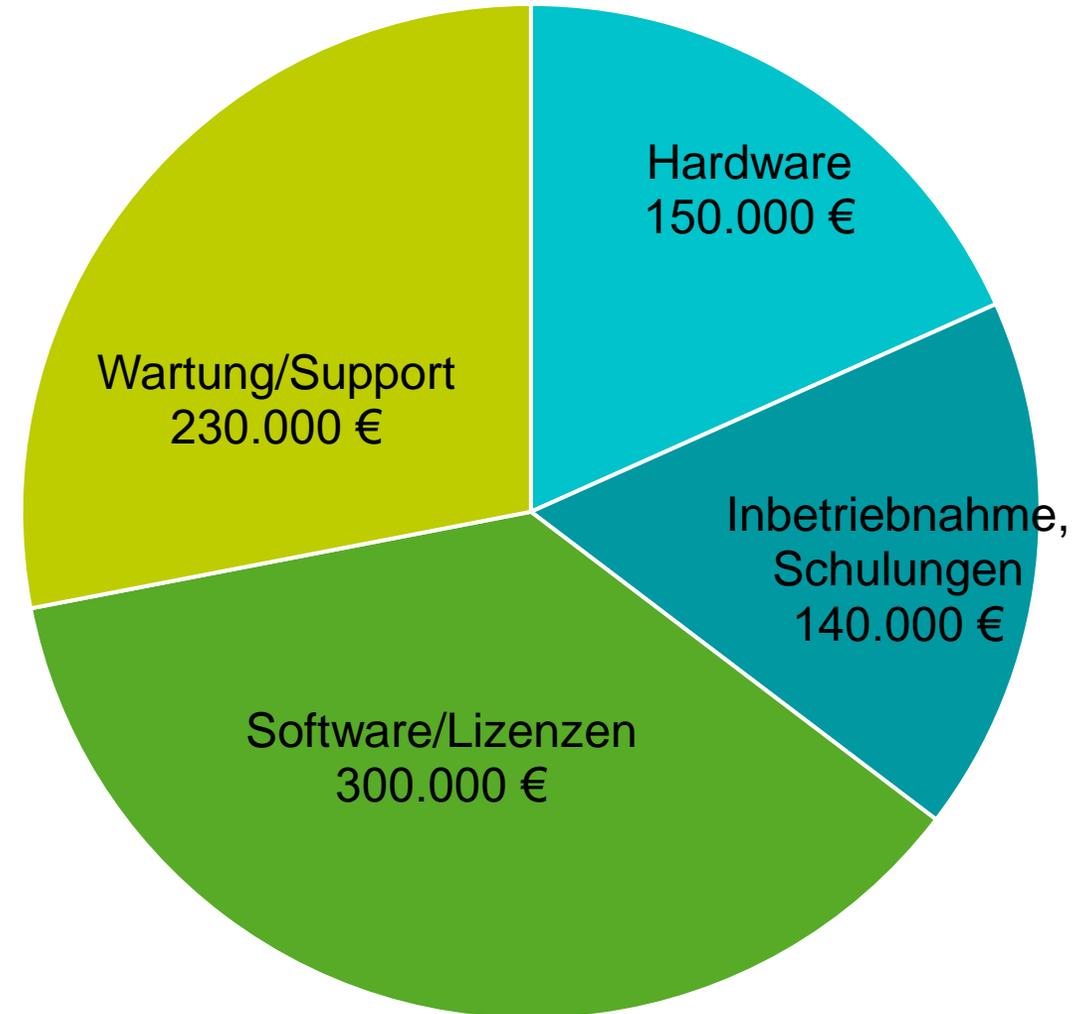
- IPv6 (!)

- per Hand zeitraubend

Beschaffung

- Landesmittel Security/Netzausbau
- Ausschreibung SIEM
- Hardware: 12 Server ~ 150 k€
- Inbetriebnahme, Schulungen: ~140 k€
- Software/Lizenzen: ~ 300 k€ für 4 Jahre
- Wartung/Support: ~ 230 k€ für 4 Jahre
- Fa. Robotron aus Dresden mit Elastic Search

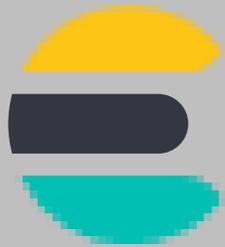
...und Sarah



ELK Stack



ELK Stack

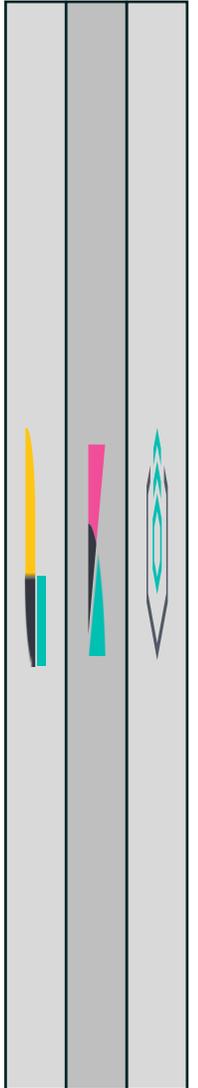


”

„Elasticsearch is a distributed, RESTful **search and analytics engine** capable of addressing a growing number of use cases. As the heart of the Elastic Stack, it **centrally stores your data** for lightning fast search, fine-tuned relevancy, and powerful analytics that scale with ease.”

- <https://www.elastic.co/elasticsearch>

”



ELK Stack

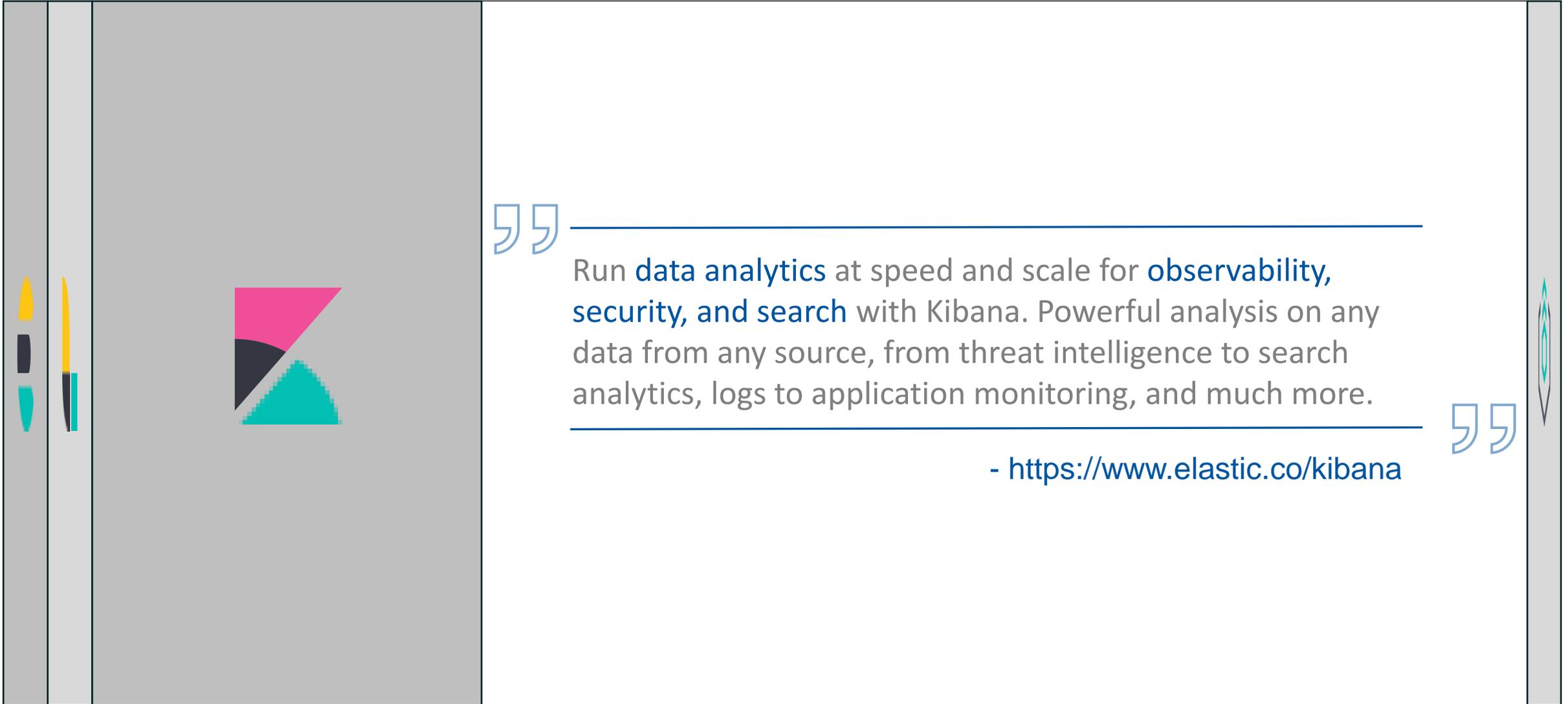
”

Logstash is a free and open server-side data processing pipeline that **ingests data** from a multitude of sources, transforms it, and then sends it to your favorite "stash."

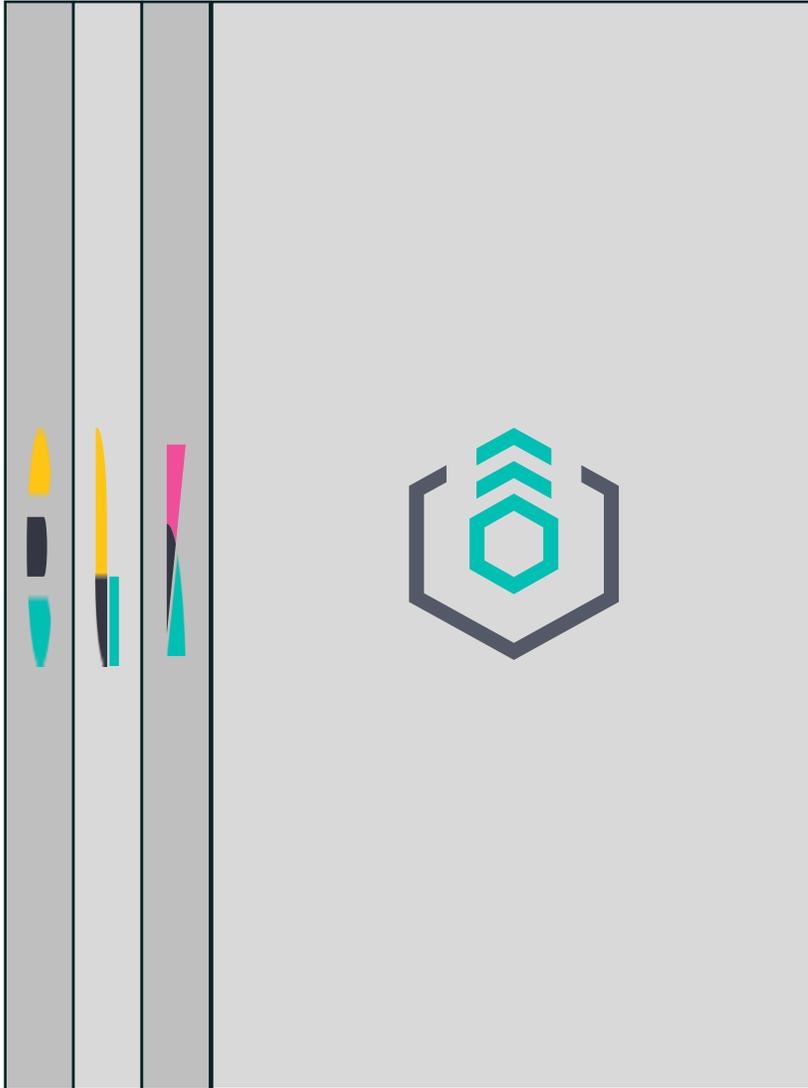
”

- <https://www.elastic.co/logstash>

ELK Stack



ELK Stack



”

“With Elastic Agent you can collect all forms of data from anywhere with a **single unified agent per host**. One thing to install, configure, and scale.”

”

- <https://www.elastic.co/elastic-agent>

Standard Features

The dashboard is divided into several sections:

- Elasticsearch Overview:** Shows system health (Healthy), version (8.12.1), uptime (a month), machine learning jobs (47), and license (Platinum, expires on April 1, 2026).
- Kibana Overview:** Shows system health (Healthy), 0 requests, max response time (0 ms), rule success ratio (99.87%), and 4 queued rules.
- Logstash Overview:** Shows 23.3b events received and 23.3b events emitted.
- Infrastructure Metrics:** A grid of charts showing metrics for various hosts, such as 23%, 22.8%, 19.7%, 17.3%, 0%, and 0%.
- Anomaly timeline:** A heatmap showing anomalies over time, sorted by max anomaly score. It includes a severity scale from 0 to 50 and a table of anomalies.
- Entity Analytics:** Shows 0 critical hosts, host risk scores (12 total), and user risk scores (16 total).

Large blue text labels are overlaid on the dashboard:

- Stack Monitoring** (over Kibana)
- Infrastructure Metrics** (over the metrics grid)
- Machine Learning** (over the anomaly timeline)
- Security** (over Entity Analytics)

Standard Features

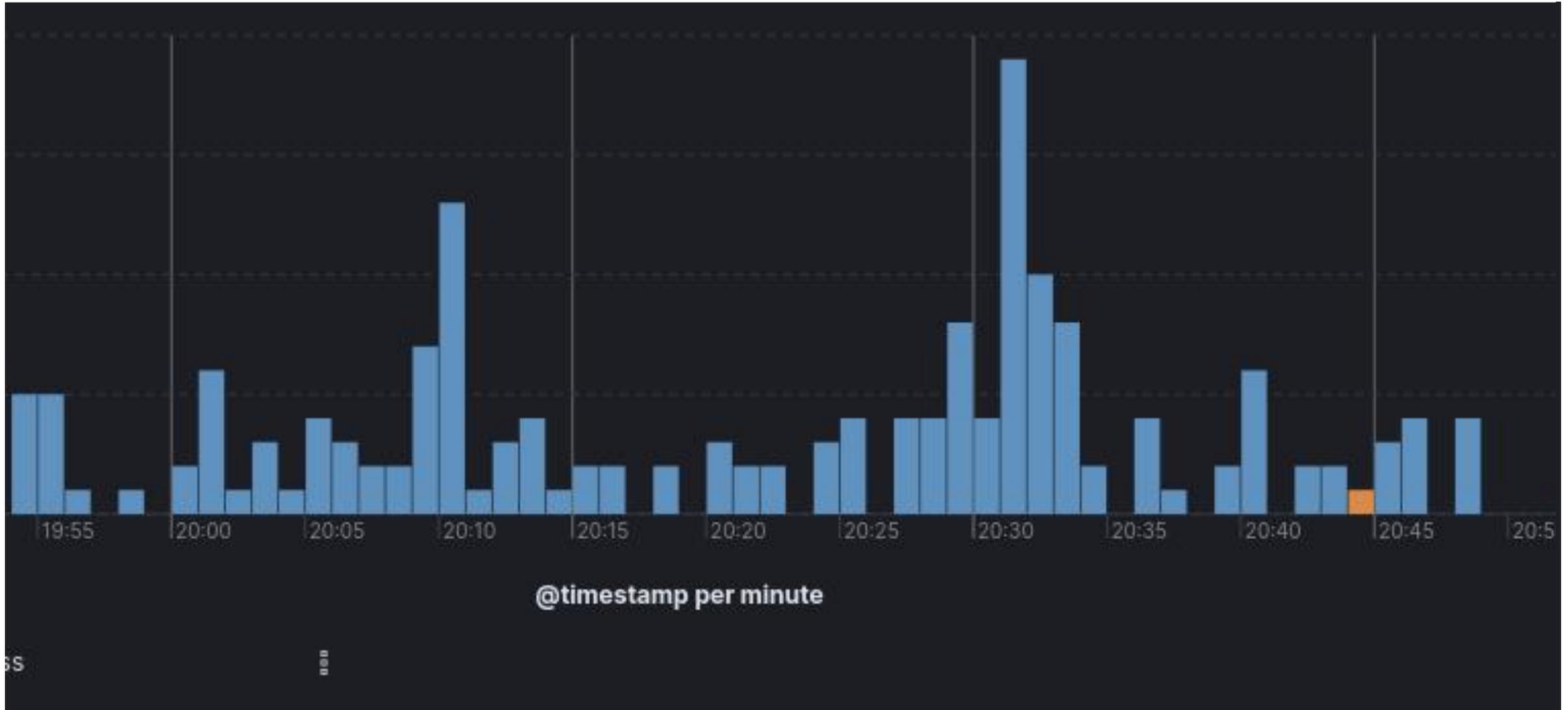
The dashboard is divided into several sections:

- Elasticsearch Overview:** Shows system health (Healthy), version (8.12.1), uptime (a month), machine learning jobs (47), and license (Platinum, expires on April 1, 2026). A red alert icon indicates 1 alert.
- Kibana Overview:** Shows system health (Healthy), 0 requests, max response time (0 ms), rule success ratio (99.87%), and 4 queued rules.
- Logstash Overview:** Shows 23.3b events received and 23.3b events emitted.
- Anomaly Heatmap:** A grid showing anomaly scores over time (March 5-8, 2024) for various hosts. A legend indicates severity levels from 0 to 50. Annotations are visible for specific events.
- Entity Analytics:**
 - Host Risk Scores:** Shows 0 critical hosts. A donut chart indicates 12 total hosts with risk levels: Unknown, Low, Moderate, High, and Critical.
 - User Risk Scores:** Shows 16 total users with risk levels: Unknown, Low, Moderate, High, and Critical.

Exchange

user.name	▼	#total	▼	↓ most recent
@telematel.com		10		Feb 25, 2024 @ 10:09:04.026
@ .rwth-aachen.de		10		Feb 26, 2024 @ 08:54:46.540
@scorace.com		10		Feb 26, 2024 @ 13:50:11.651
@rwth-aachen.de		10		Feb 26, 2024 @ 13:25:29.264
@rwth-aachen.de		10		Feb 26, 2024 @ 08:57:52.177
		10		Feb 26, 2024 @ 11:08:19.991
@rwth-aachen.de		10		Feb 26, 2024 @ 13:31:46.600

Exchange



Exchange

Credential Stuffing

Beispiel mit einzelner Source IP

Oft wenige Stunden, aber ~100-1000 verschiedene Usernames

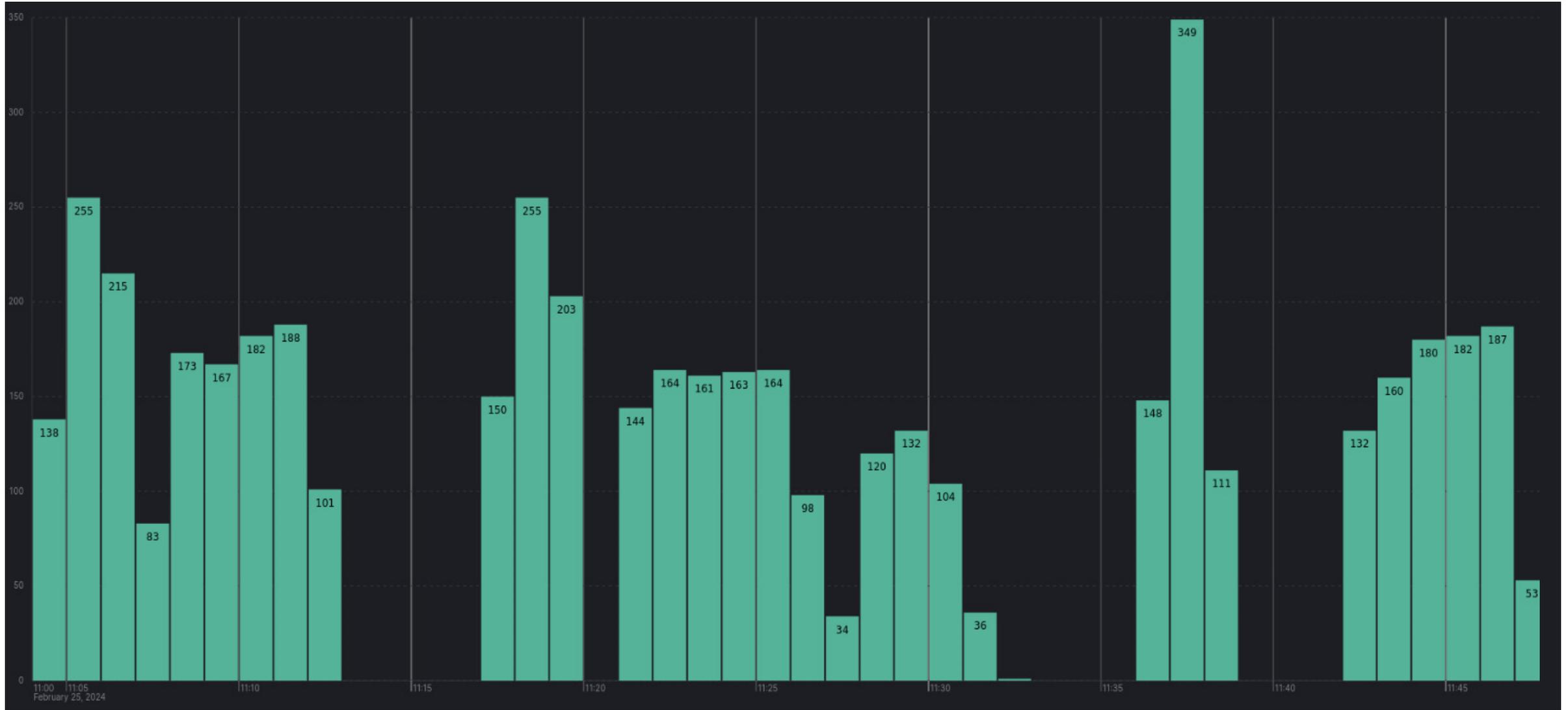
Selten erfolgreich

Low Prio Alert: viele Fails für viele Usernames

High Prio Alert: bereits auffällige IP hat erfolgreichen Login

@timestamp per minute

Exchange



Exchange

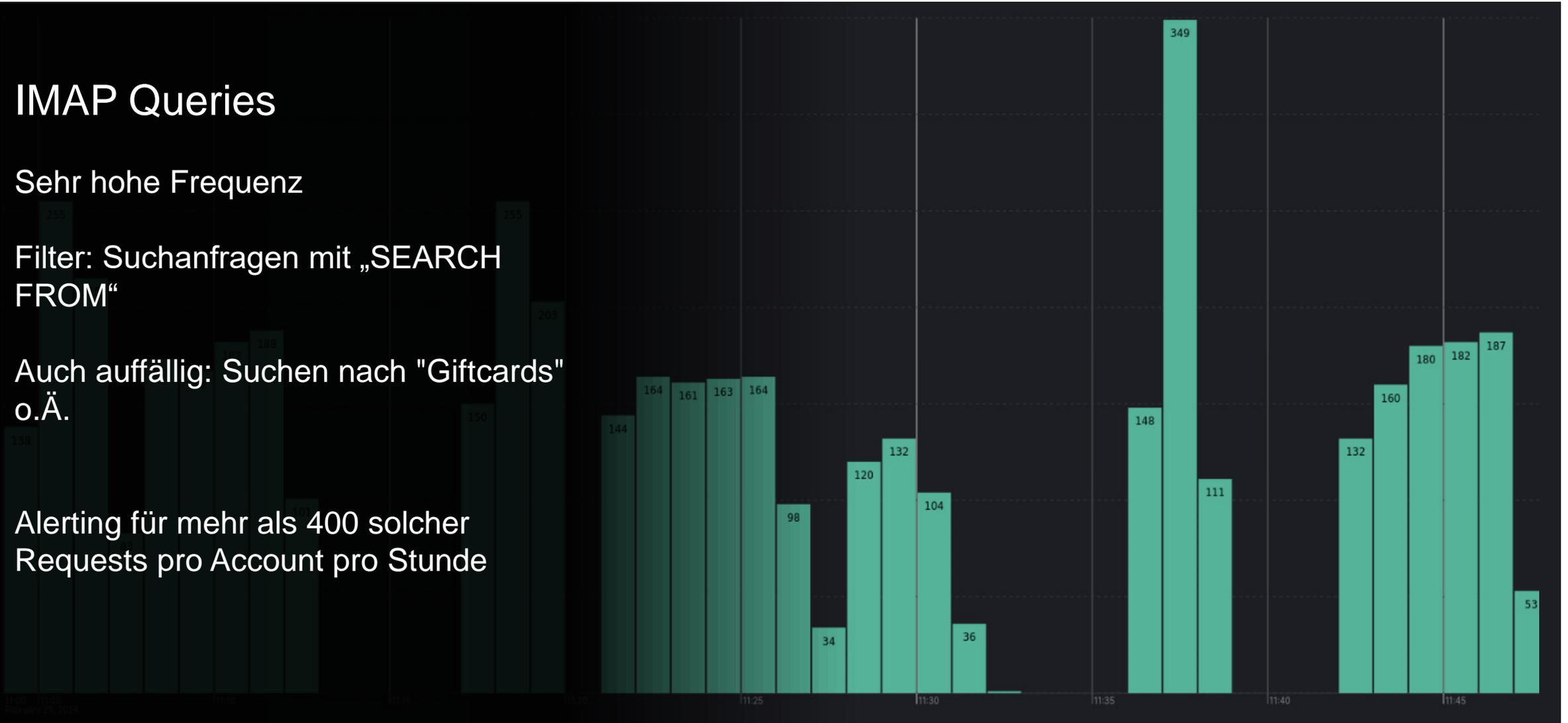
IMAP Queries

Sehr hohe Frequenz

Filter: Suchanfragen mit „SEARCH FROM“

Auch auffällig: Suchen nach "Giftcards" o.Ä.

Alerting für mehr als 400 solcher Requests pro Account pro Stunde



IMAP Queries

Sehr hohe Frequenz

Filter: Suchanfragen mit „SEARCH FROM“

Auch auffällig: Suchen nach "Giftcards" o.Ä.

Alerting für mehr als 400 solcher Requests pro Account pro Stunde

```
SEARCH FROM "giftcards@ernestjones.co.uk"
SEARCH FROM "giftcards.woolworths.com.au"
SEARCH FROM "everydaygiftcards.com.au"
SEARCH FROM "gift-noreply@pizzaexpress.com"
SEARCH FROM "donotreply@giftcards.chase.com"
SEARCH FROM "customerservices@argosgiftcards.co.uk"
SEARCH FROM "customerservice@giftcardmall.com"
SEARCH FROM "giftcards@argos.co.uk"
SEARCH (FROM "email-puma.com") (BODY "gift card from your")
SEARCH FROM "@giftnix.com"
SEARCH FROM "airbnbuk@launchgiftcards.com"
SEARCH FROM "@sgiftcard.eu"
SEARCH FROM "checkout@giftcardmall.finish-order.com"
SEARCH FROM "alerts@yougotagift.com"
SEARCH FROM "giftcard@rei.com"
SEARCH FROM "gift@yougotagift.com"
SEARCH FROM "giftcards@kroger.com"
SEARCH FROM "giftcards@bidali.com"
```

Enrichment

Netzwerkeigenschaften:		0	Mar 15, 2024 @ 09:06:37.000	@rwth.edufi.de	134.61.164.9
Name	eduroam	0	-	@rwth.edufi.de	134.61.155.222
BridgeDomain	BD-777	0	Mar 15, 2024 @ 09:38:51.000	@rwth.edufi.de	134.61.165.37
Netzwerk	134.61.128.0/18				
Netze in gleicher BridgeDomain				@rwth.edufi.de	134.61.136.111
Netzmaske	255.255.192.0	0	Mar 15, 2024 @ 10:24:35.000	@rwth.edufi.de	134.61.135.99
Gateway	134.61.128.1 (Pin)	0	Mar 15, 2024 @ 11:46:11.000	@rwth.edufi.de	134.61.165.35
VLAN	777 (Network-Topo)				
Router	c8500-wlan-1 (2a0)	0	Mar 15, 2024 @ 09:51:04.000	@rwth.edufi.de	134.61.138.212
zusätzlicher Router					

134.61.165.111

Enrichment

Mar 15, 2024 @ 09:06:17.000	Mar 15, 2024 @ 09:06:37.000	@rwth.edufi.de	134.61.164.9	[2a00:8a60:c000:1:3f21:30d6:8fe9:b192, 2a00:8a60:c000:1:90a9:4aff:fe27:580, 2a00:8a60:c000:1:e897:25a:c99e:8fbe, ...
Mar 15, 2024 @ 09:06:17.000	-	@rwth.edufi.de	134.61.155.222	fe80::1850:175f:a596:cd71
Mar 15, 2024 @ 09:06:17.000	Mar 15, 2024 @ 09:38:51.000	@rwth.edufi.de	134.61.165.37	[2a00:8a60:c000:1:474:fdb0:737a:4847, 2a00:8a60:c000:1:35:a321:9a67, fe80::44b:f600:0000:0000]
Mar 15, 2024 @ 09:06:16.000	-	@rwth.edufi.de	134.61.136.111	[2a00:8a60:c000:1:7c95:d462:a589:bcad, 2a00:8a60:c000:1:f860:589f:ce4b:754e, fe80::1f4d:328e:f0e1:7b91]
Mar 15, 2024 @ 09:06:16.000	Mar 15, 2024 @ 10:24:35.000	@rwth.edufi.de	134.61.135.99	[2a00:8a60:c000:1:dd07:ea8e:1f9d:ce20, fe80::c09d:d5ff:fe5f:b1f3]
Mar 15, 2024 @ 09:06:16.000	Mar 15, 2024 @ 11:46:11.000	@rwth.edufi.de	134.61.165.35	[2a00:8a60:c000:1:411:7c35:5537:a53, fe80::844:c5c3:3c4b:a75d]
Mar 15, 2024 @ 09:06:16.000	Mar 15, 2024 @ 09:51:04.000	@rwth.edufi.de	134.61.138.212	[2a00:8a60:c000:1:894:964e:e8bd:777c, fe80::907:fb4a:66dd:f94c]

Start

Stop

User

IPv4

IPv6

Fazit

- Mittlerweile erste Alarme aus dem SIEM (auch in Webex)
- Exchange „geknackt“
- Work in Progress

**Vielen Dank
für Ihre Aufmerksamkeit**