Chancen der Gefahrenerkennung mit einem SIEM System

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

IT Center | RWTH AACHEN UNIVERSITY

Agenda

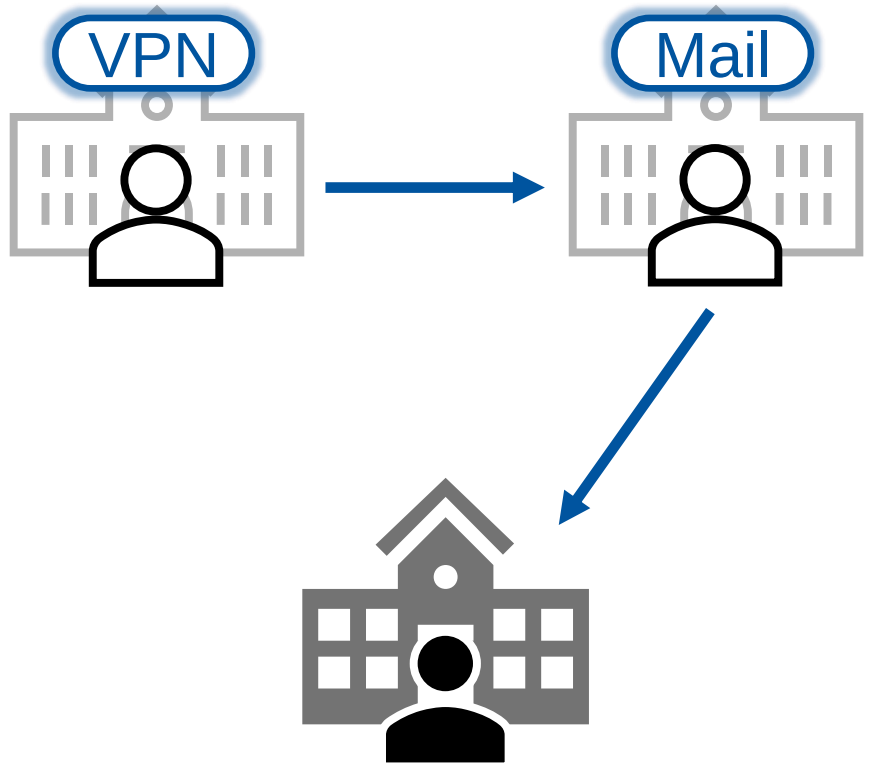
- Aktuelle Situation
- Beschaffung
- ELK Stack
- Beispiele mit Exchange Daten
- Enrichment

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

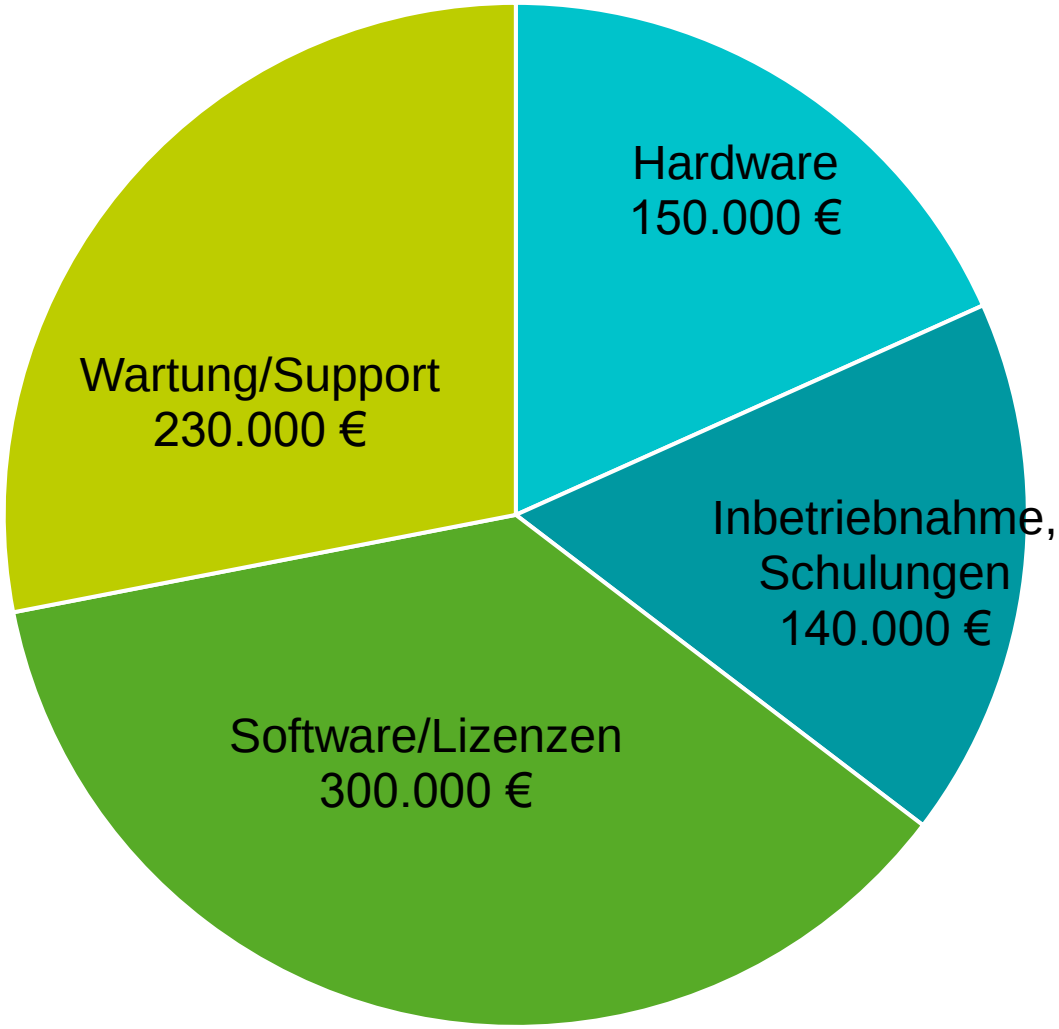
- Landesmittel Security/Netzausbau

- 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

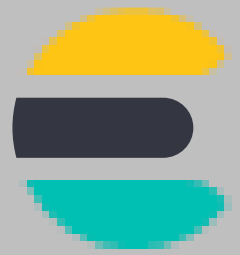
- Fa. Robotron aus Dresden mit Elastic Search

…und Sarah



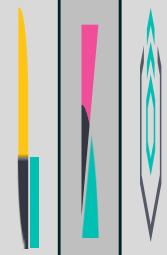
ELK Stack

ELK Stack

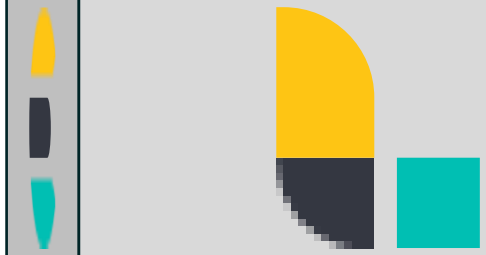


„Elasticsearch is a distributed, RESTful search and analytics engine capable of addressing a growing number of use cases. As the heart of the Elastic Stack, it centrally stores your data for lightning fast search, fine-tuned relevancy, and powerful analytics that scale with ease.”

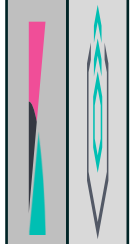
- https://www.elastic.co/elasticsearch



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

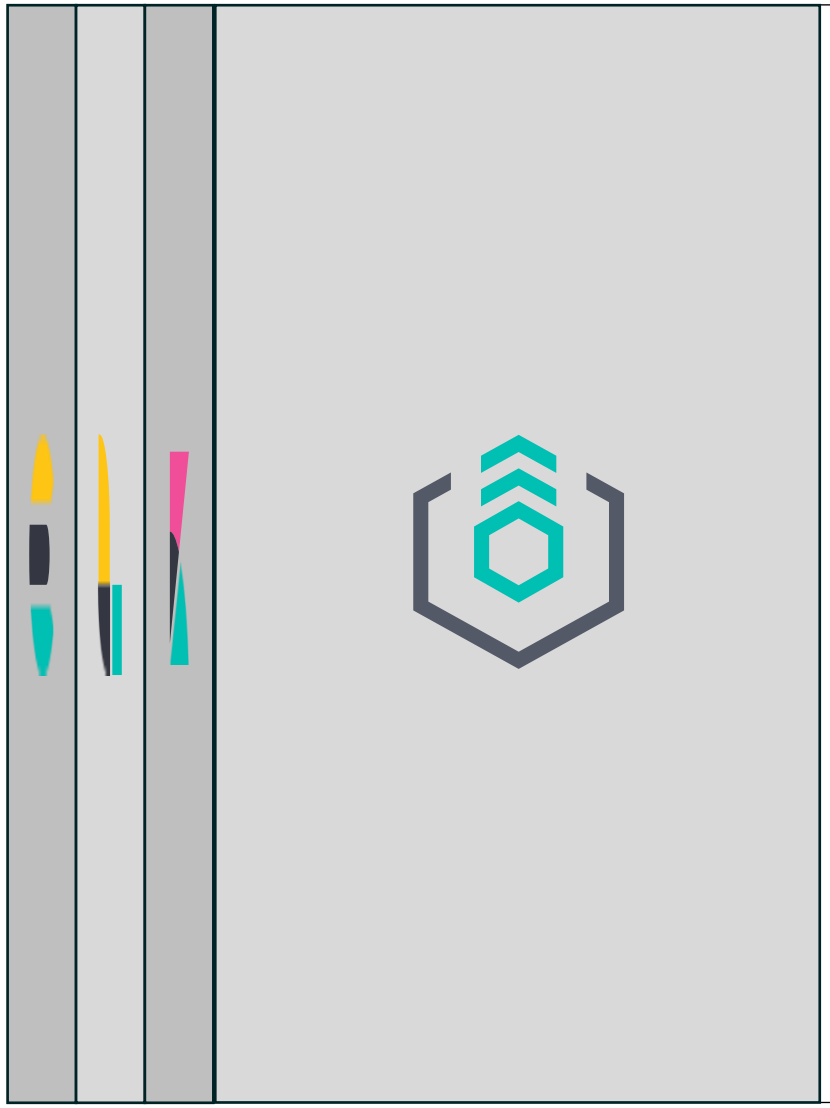


ELK Stack

Run data analytics at speed and scale for observability, security, and search with Kibana. Powerful analysis on any data from any source, from threat intelligence to search analytics, logs to application monitoring, and much more.

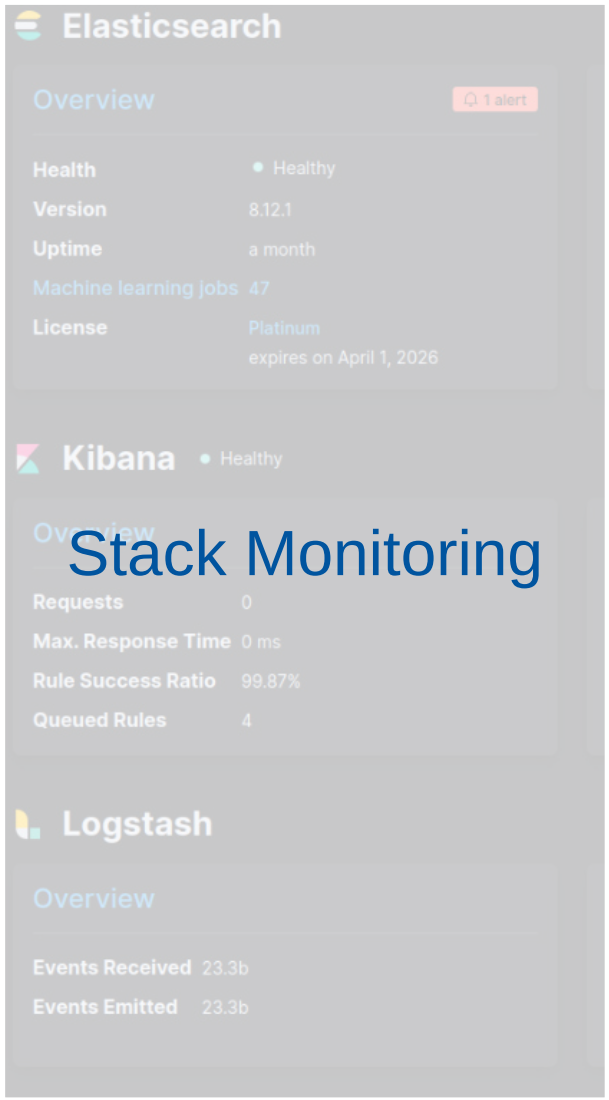
- https://www.elastic.co/kibana

ELK Stack

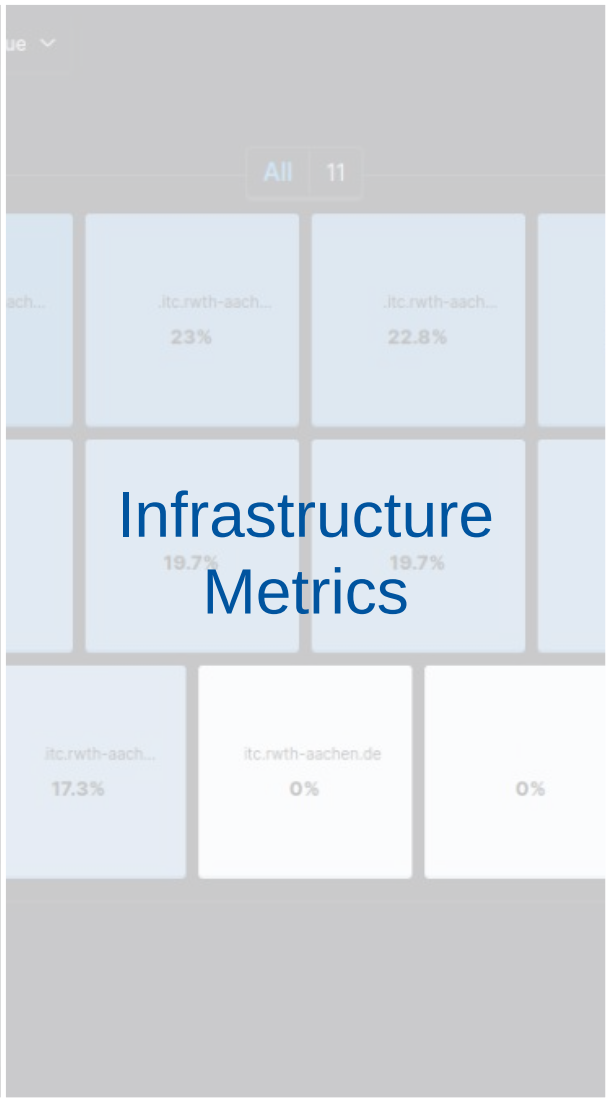


> “With Elastic Agent you can collect all forms of data from anywhere with a single unified agent per host. One thing to install, configure, and scale.“
>
> - https://www.elastic.co/elastic-agent

Standard Features

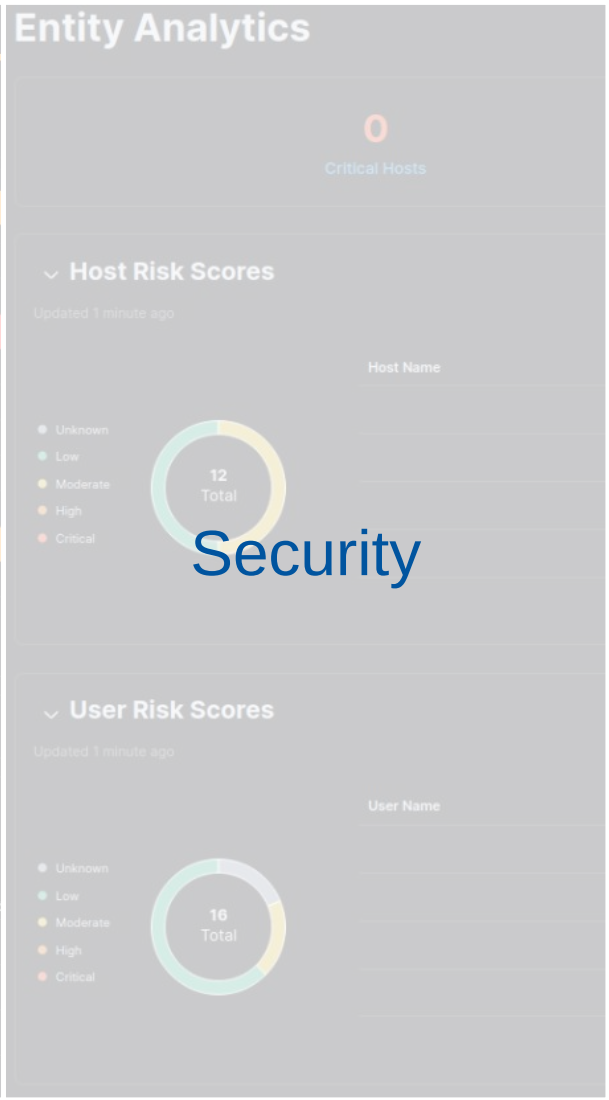


Stack Monitoring



Infrastructure Metrics

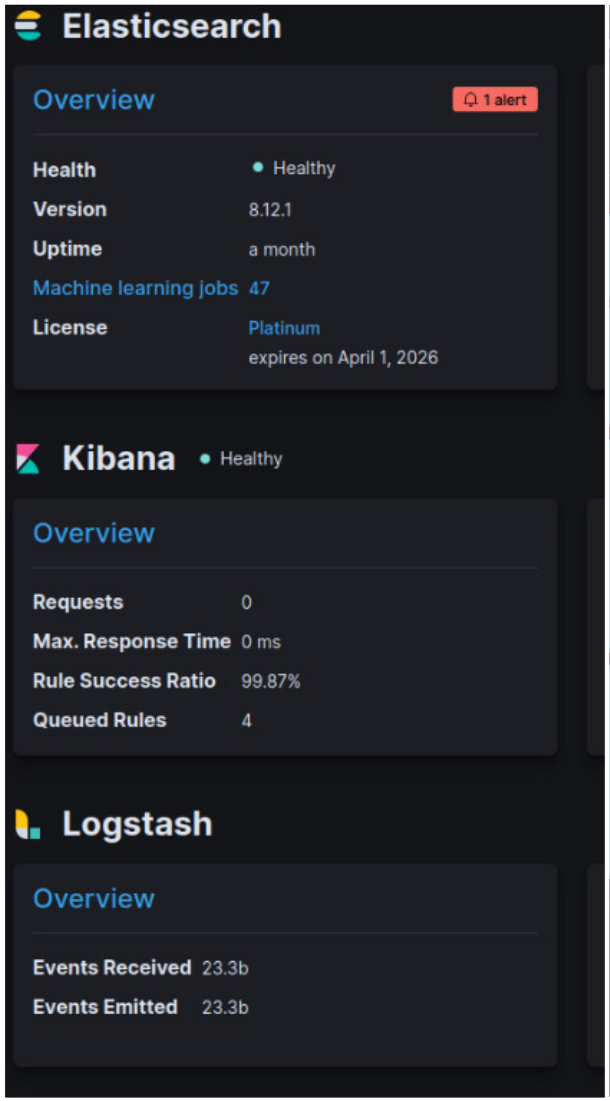
Machine Learning

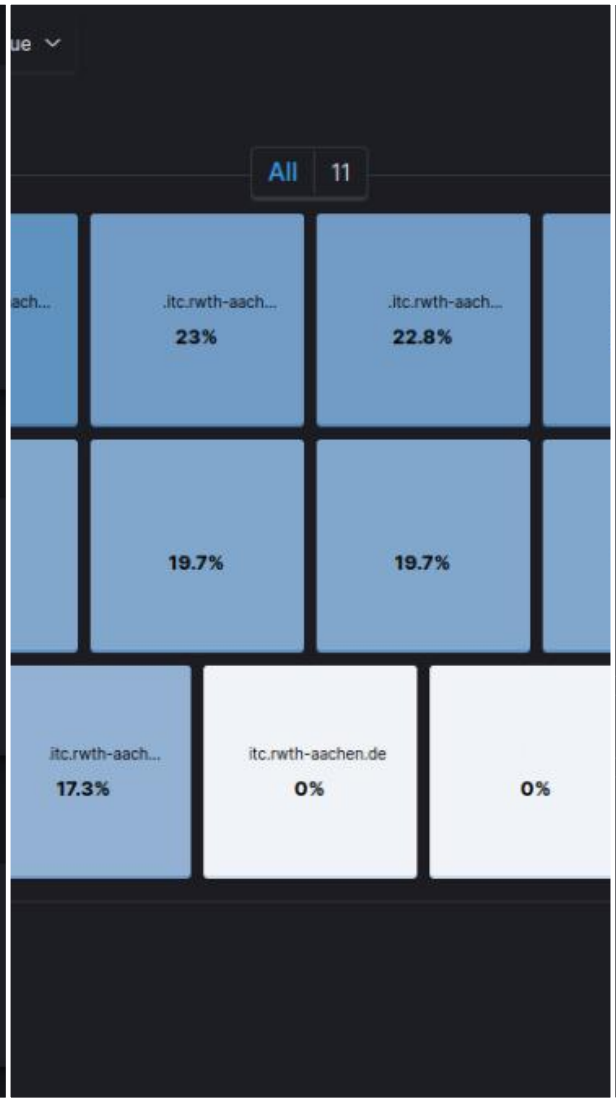


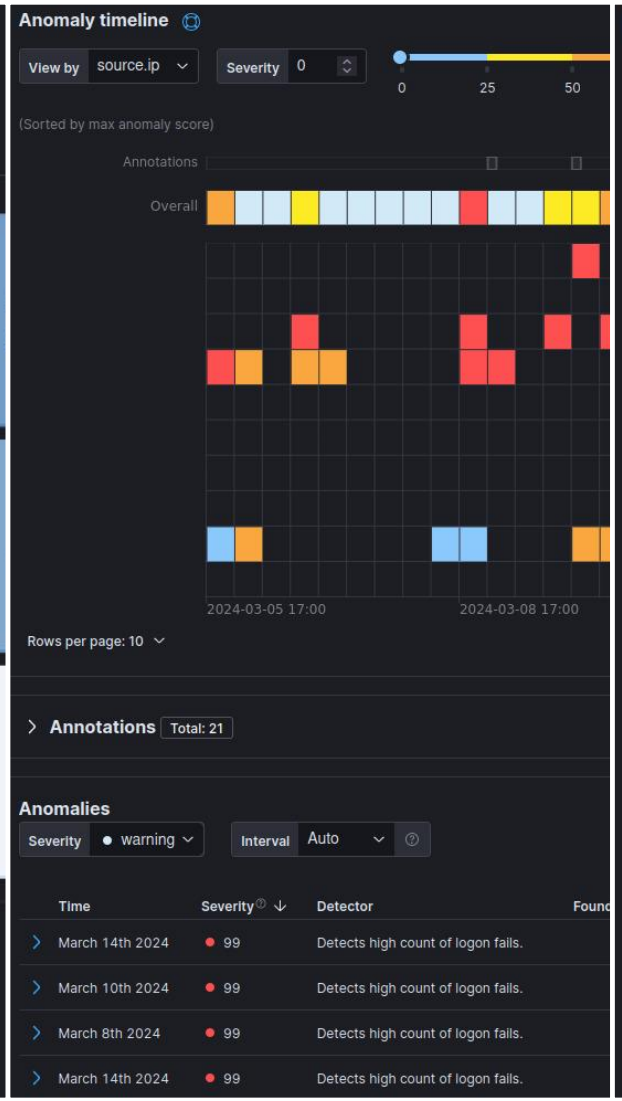
Security

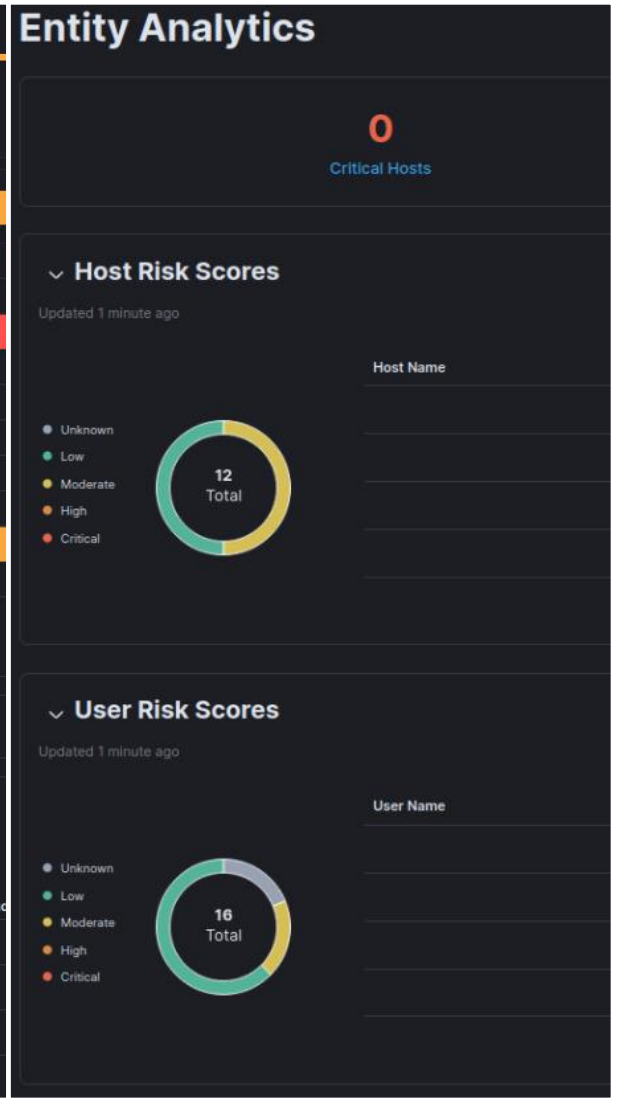
IT Center | RWTH AACHEN UNIVERSITY

Standard Features





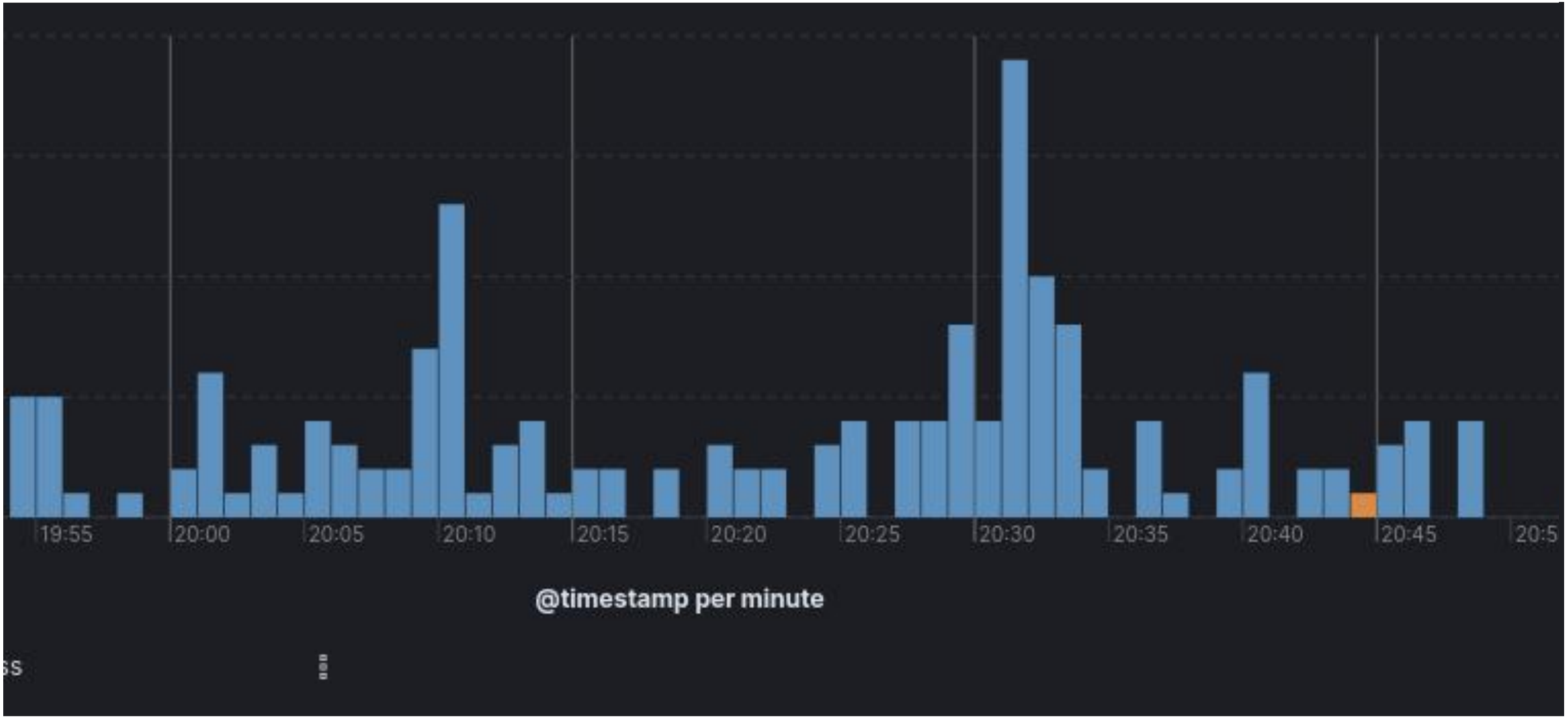




Exchange

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


19:55
20:00
20:05
20:10
20:15
20:20
20:25
20:30
20:35
20:40
20:45
20:5
@timestamp per minute

Exchange

Credential Stuffing

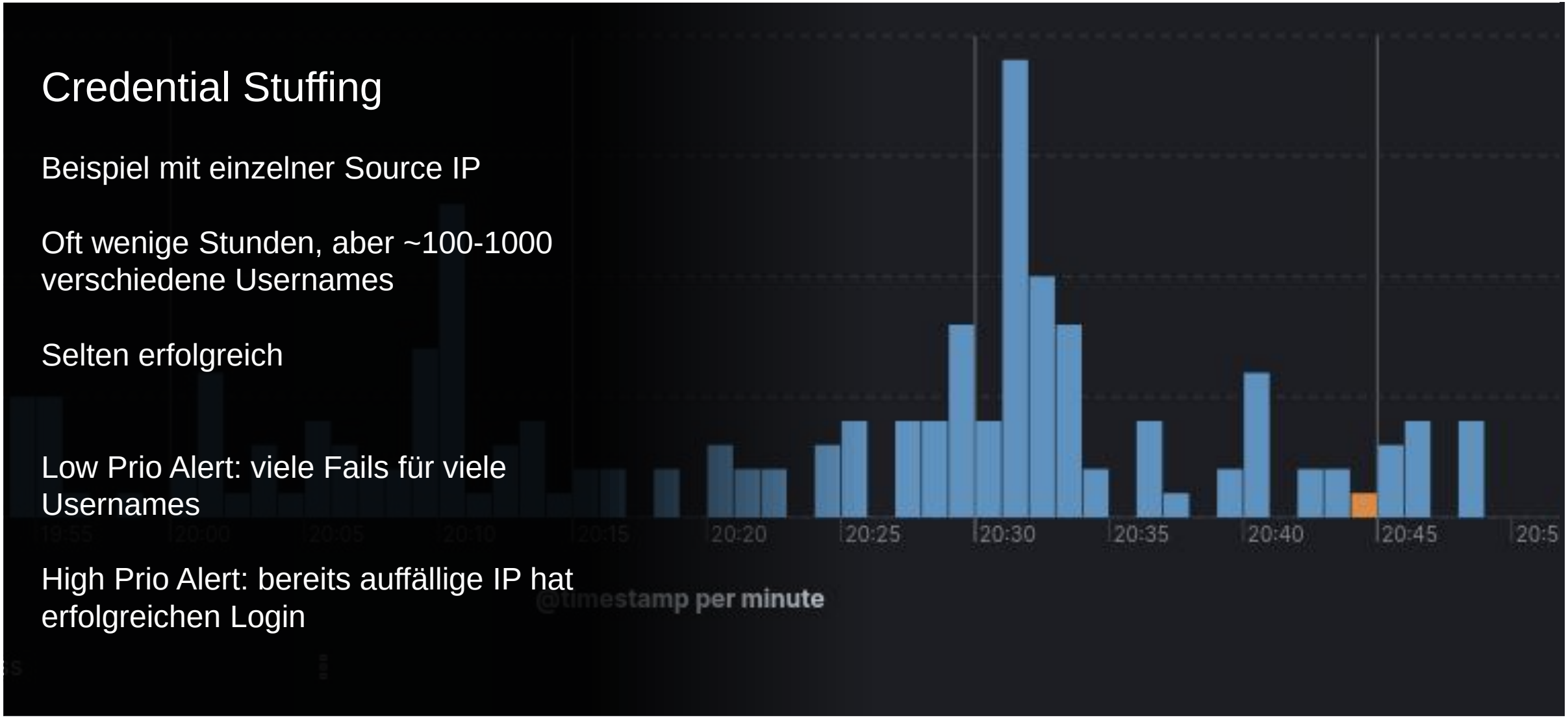
Beispiel mit einzelner Source IP

Oft wenige Stunden, aber ~100-1000 verschiedene Usernames

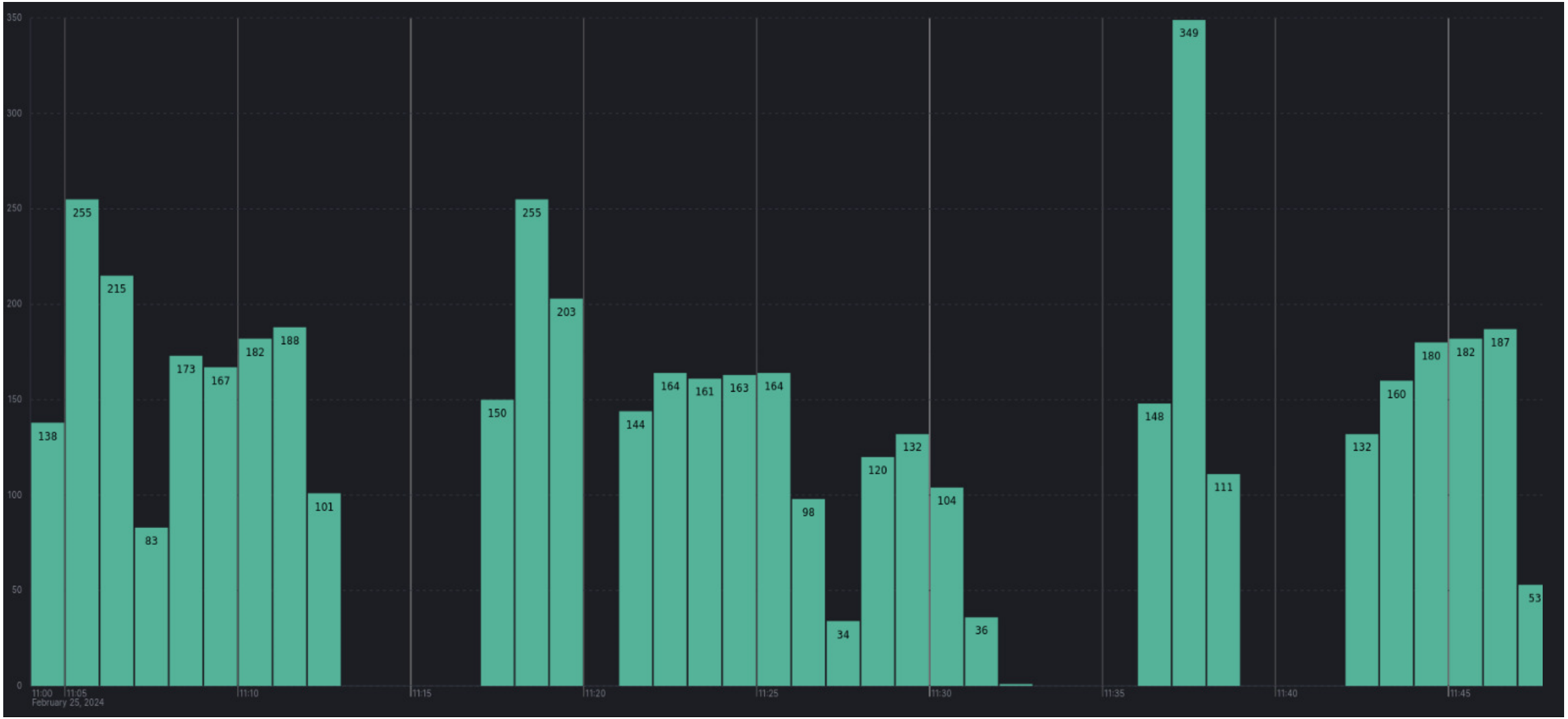
Selten erfolgreich

Low Prio Alert: viele Fails für viele Usernames

High Prio Alert: bereits auffällige IP hat erfolgreichen Login



Exchange



IT Center | RWTH AACHEN UNIVERSITY

Exchange

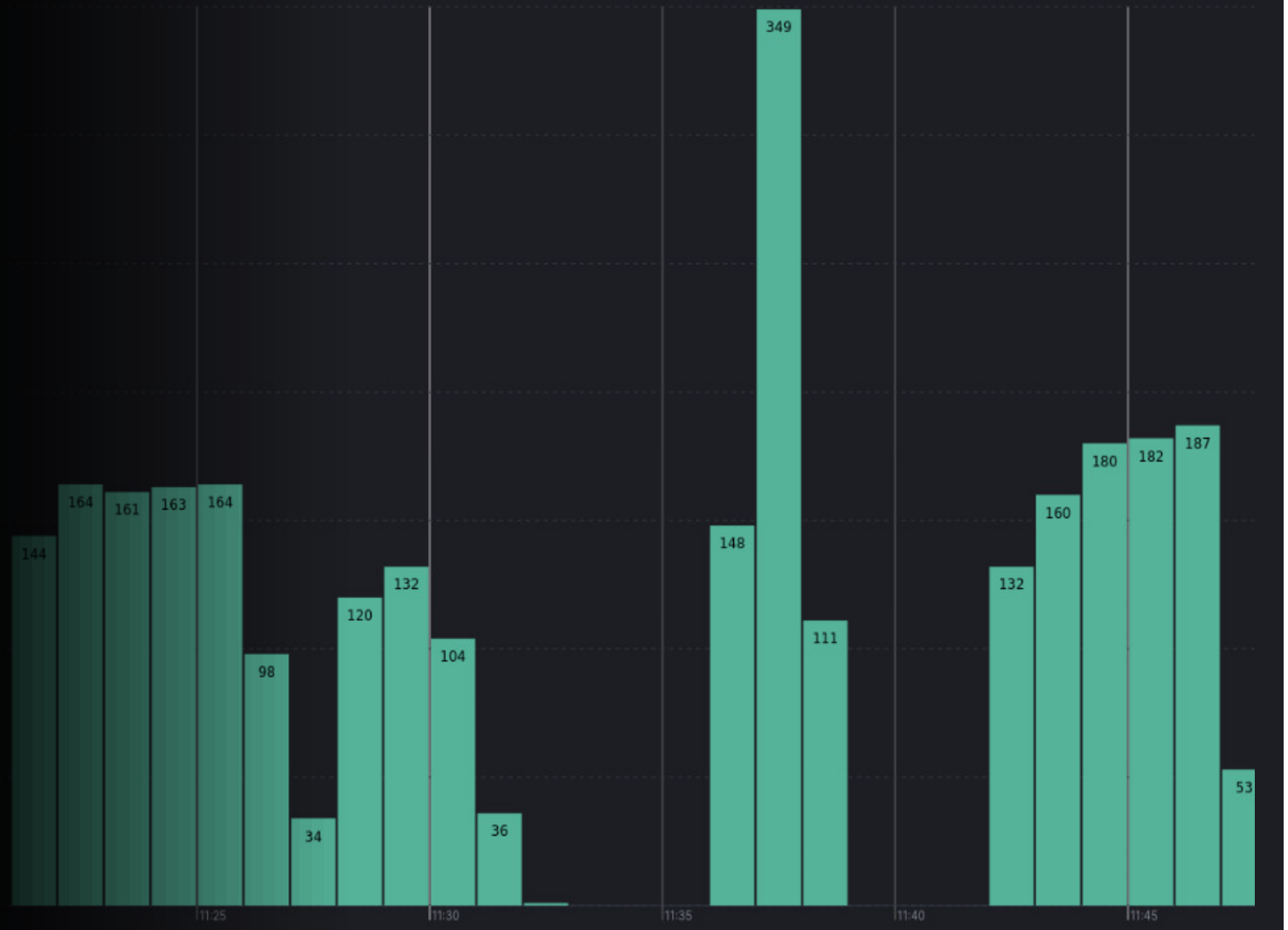
IMAP Queries

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



Exchange

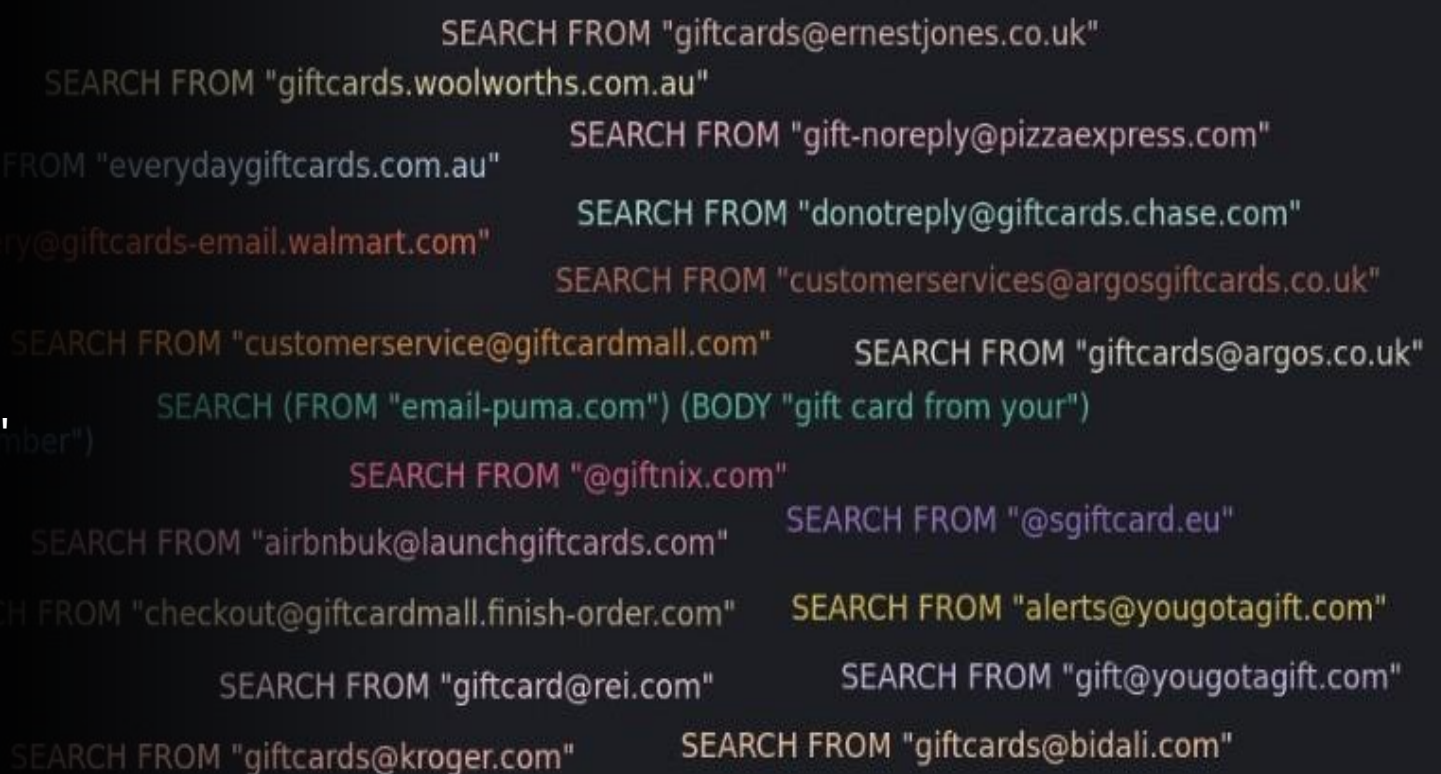
IMAP Queries

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



Enrichment

Netzwerkeigenschaften:	
Name	eduroam
BridgeDomain	BD-777
Netzwerk	134.61.128.0/18
Netze in gleicher BridgeDomain	
Netzmaske	255.255.192.0
Gateway	134.61.128.1 (Pin
VLAN	777 (Network-Topo
Router	c8500-wlan-1 (2a(
zusätzlicher Router	

134.61.165.111

0	Mar 15, 2024 @ 09:06:37.000	@rwth.edufi.de	134.61.164.9
0	-	@rwth.edufi.de	134.61.155.222
0	Mar 15, 2024 @ 09:38:51.000	@rwth.edufi.de	134.61.165.37
		@rwth.edufi.de	134.61.136.111
0	Mar 15, 2024 @ 10:24:35.000	@rwth.edufi.de	134.61.135.99
0	Mar 15, 2024 @ 11:46:11.000	@rwth.edufi.de	134.61.165.35
0	Mar 15, 2024 @ 09:51:04.000	@rwth.edufi.de	134.61.138.212

Enrichment

Start	Stop	User	IPv4	IPv6
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:c0…35:a321:9a67, fe80::44b:f6…
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::807:fb4a:66dd:f94c]

Fazit

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

Vielen Dank
für Ihre Aufmerksamkeit