HBO max

DTC Security

Advanced Signal Sciences Investigation/Blocking

01 December 2021

Agenda

Not-so-clean blocks

Last time we just looked at “happy path”

“The QA environment is broken!”

*Or, how to tell if *we’re* blocking something*

“What are all these 403s”

When your starting point is just request count of certain statuses…

Q&A

Not-so-clean blocks

- **Success rate is suspiciously high for a given header order**
  - Subjective but let's say north of 5%
    - What paths are they hitting?
    - What do User-Agents look like?
      - Do not make decisions off UA alone though
    - LOGINATTEMPT-tagged traffic versus not
    - Are compromised usernames being hit an outsized number of times to obfuscate "true" success rate?
    - Follow traffic all the way to other supporting logs
      - Such as reCAPTCHA or tokens

“The QA environment is broken!”

- **Need (IP address OR username) and approx. timestamp at a minimum**

- **Is traffic showing up in Signal Sciences?**
  - Not blocked by Fastly then
    - Decreasingly relevant but still
  - Response code 403 typically suggests Magellan denial
    - MaxMind geo, MaxMind VPN, or ASN block that differed from Fastly edge

- **index=*prod* <IP_ADDRESS_OR_OTHER_IDENTIFIER_HERE> for HBO Splunk**
  - **Example Splunk via Slack thread**
  - Some **Kibana starters** too
  - Just throw the unique string on the end in both cases, basically

Smart device client

Billions of daily requests

fastly

comet.api.hbo.com
gateway.api.hbo.com
(*N* variations …)

Signal Sciences

WAF

Tokens service

reCAPTCHA Enterprise

User table

Android & iOS

Mobile client

reCAPTCHA Enterprise

play.hbomax.com

www.hbomax.com

Web browsers

Millions of daily requests

fastly

commerce-experience.api.hbo.com

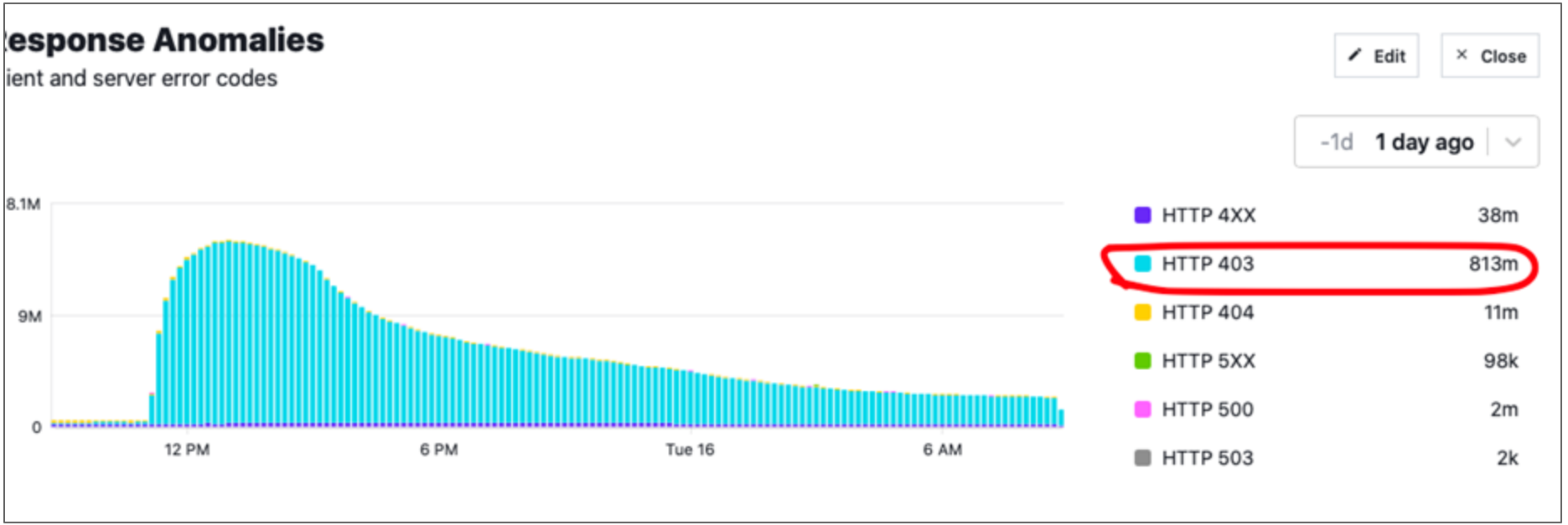
AWS WAF

Buy flow login service

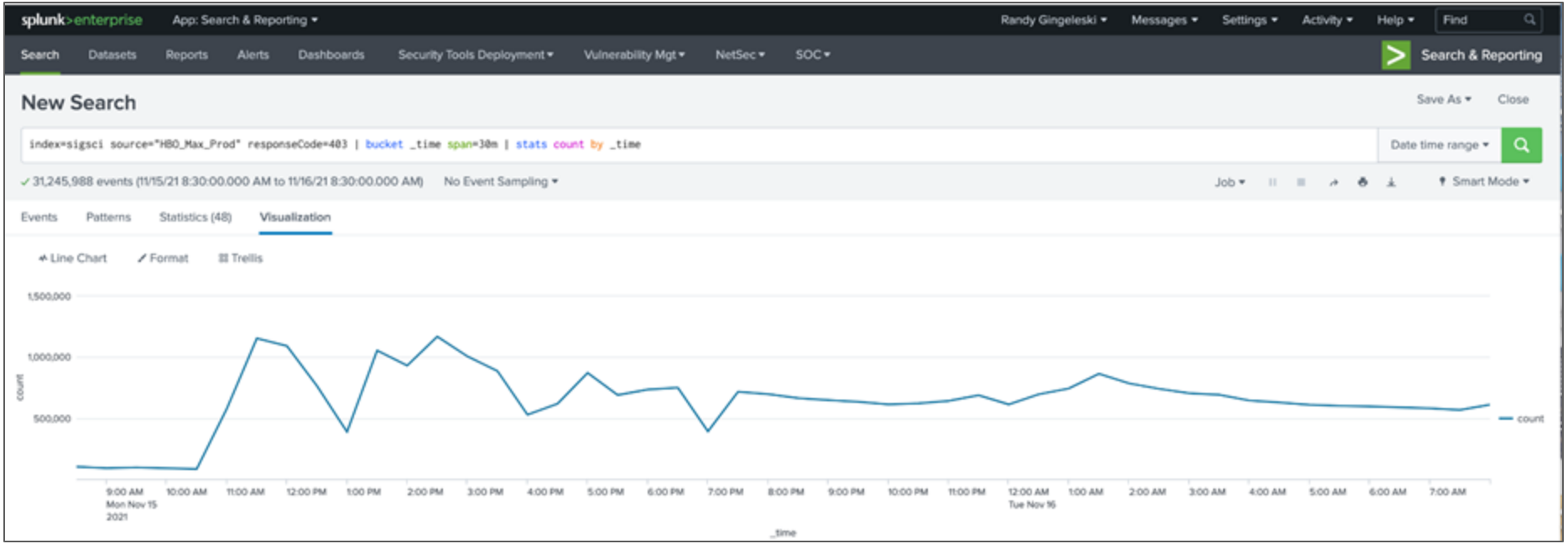
reCAPTCHA Enterprise

reCAPTCHA Enterprise

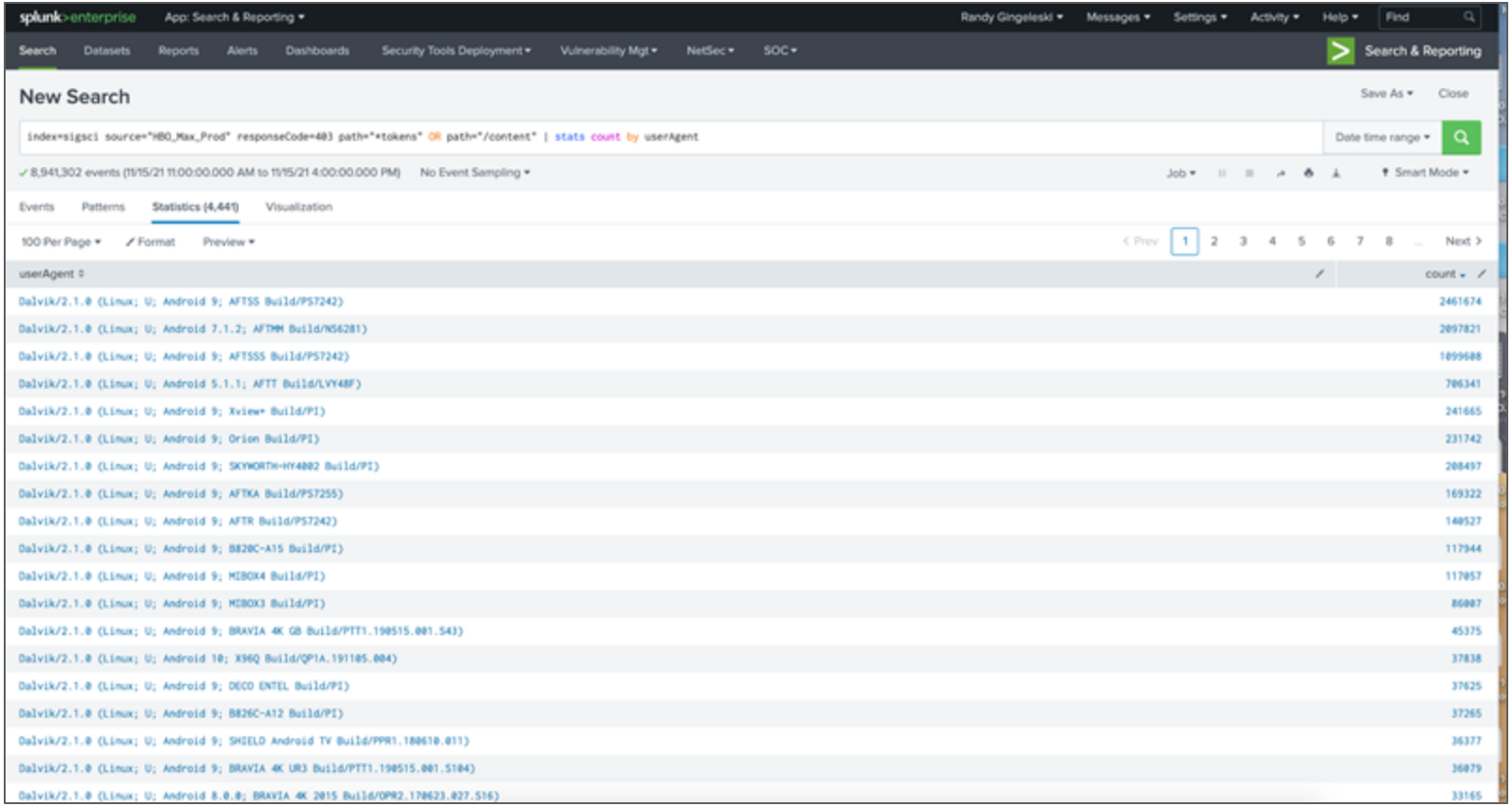
“What are all these 403s”



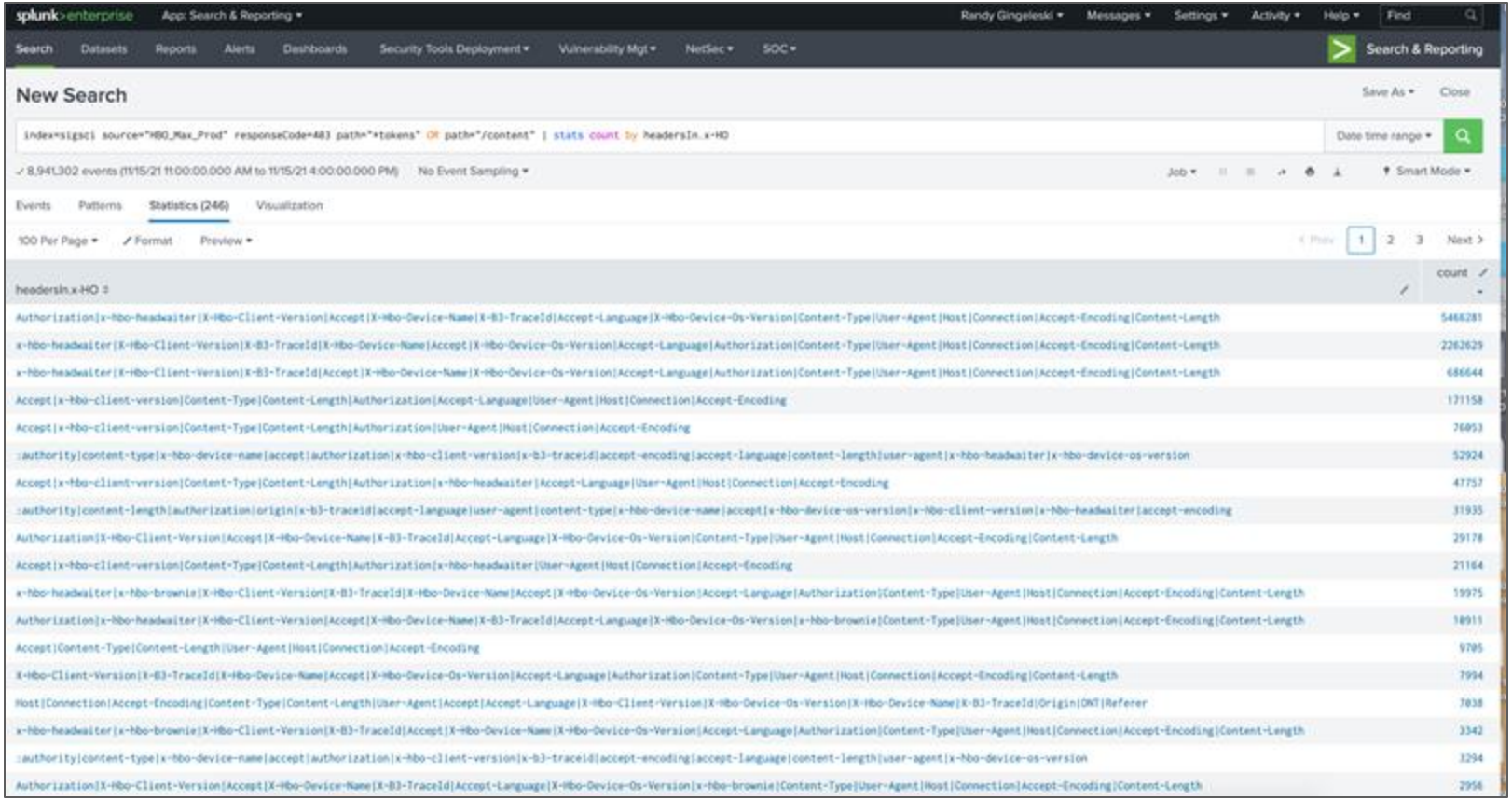
“What are all these 403s”



“What are all these 403s”



“What are all these 403s”



Questions?