Piegādes ķēžu uzbrukumi

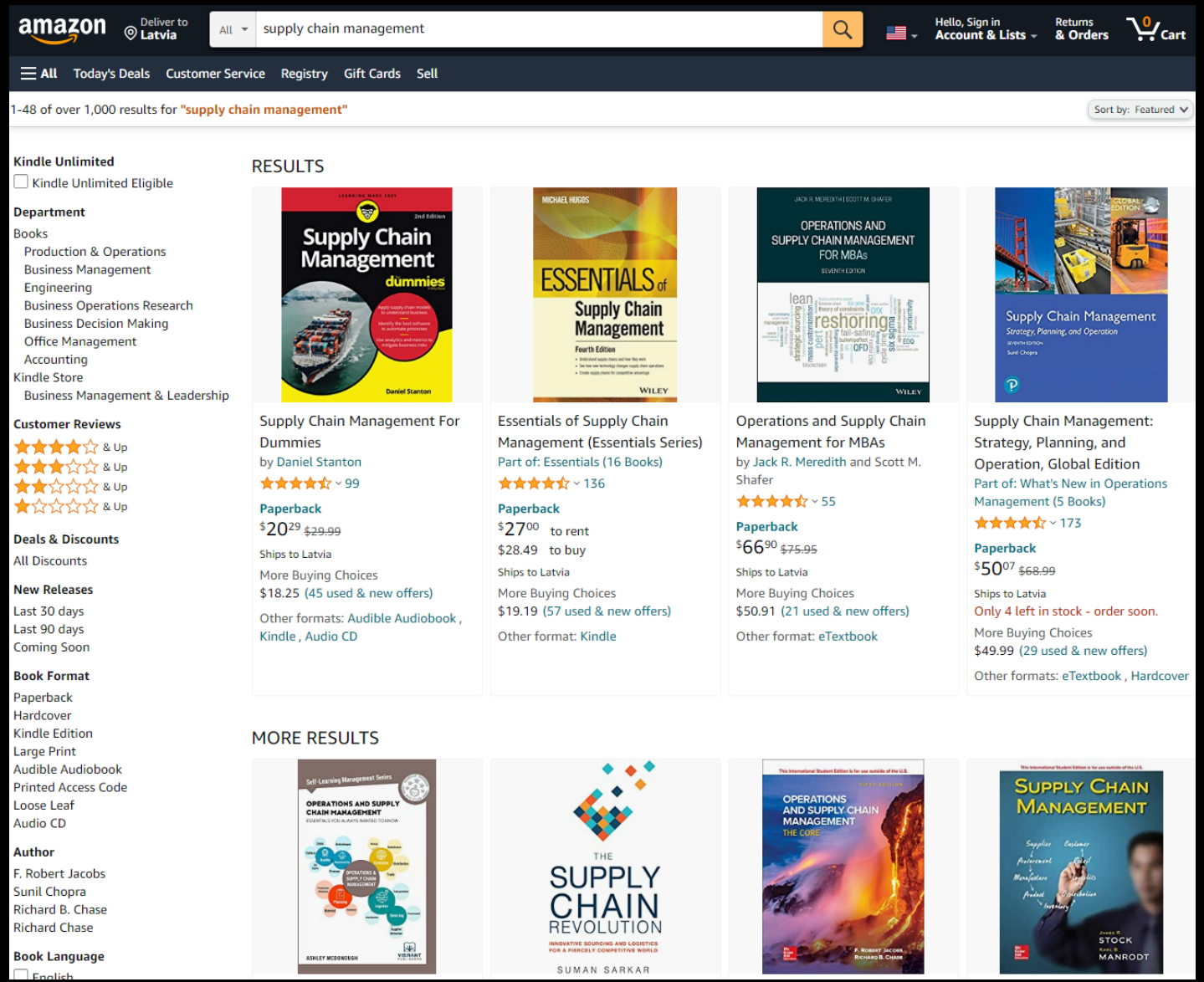
Andrejs Konstantinovs

CERT.LV, 24.03.2022

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Satura rādītājs

Kas ir piegādes ķēdes



IT piegādes ķēžu piemēri

- Programmas (un programmas komponenšu) ražotājs
  - Microsoft
- Aparatūras ražotājs
  - Cisco
  - MikroTik
- Mākoņpakalpojumu uzturētājs
- Ārpakalpojumi
  - Epastu uzturētājs
  - Grāmatvedības sistēmas uzturētājs
  - Mājaslapas uzturētājs
- Drošības risinājumu (appliances) ražotājs
  - Ubiquity
  - Fortinet

Piegādes ķēžu riski

- **Var tikt ietekmēta uzņēmuma / organizācijas darbība**
- **Ražotais produkts var būt ievainojams**
- **Var tikt atklāti, nozaudēti vai modificēti klientu dati**
- **Piedāvātais serviss var papildus risku klientiem**

NotPetya (2017)

2016: Petya (ransowmare)

14.04.2017: EternalBlue (NSA)

12.05.2017: WannaCry (worm)

27.06.2017: NotPetya

M.E.Doc – Ukrainas grāmatvedības programmatūra

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

https://www.flickr.com/photos/68359921@N08/48489922737

SolarWinds (2020)

2019. gada septembris – SolarWinds infrastruktūras haks
2020. gada marts – trojanizēti SolarWinds atjauninājumi
2020. gada decembris – FireEye atklāj, ka ir uzlauzti

Rezultāts:

- **200 organizācijas uzlauztas**
- **18000 – organizāciju skaits, kas saņēmuši trojānu**
- **33000 – SolarWinds Orion lietotāju skaits**

Dependency Confusion (2021)

lekšēju bibliotēku aizvietošana ar ārējām:

- **Python**
- **NPM**
- **Ruby**
- **Maven**
- **Gradle**
- **NuGet**

https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610
https://azure.microsoft.com/en-us/resources/3-ways-to-mitigate-risk-using-private-package-feeds/

Microsoft Exchange (2021)

05.01.2021: DEVCORE informē Microsoft par atklātajiem 0day

06.01.2021: pirmais zināmais incidents

28.02.2021: automatizēts ekspluatēšanas vilnis

02.03.2021: Microsoft publicē ielāpus

Skartas MS Exchange 2010, 2013, 2016, 2019 versijas

Kaseya (2021)

Kaseya VSA:

- **attālināta monitoringa un menedžmenta rīks**
- **populārs «managed service providers» vidē**
- **ievainojamība ļāva apiet autentifikāciju VSA portālā**

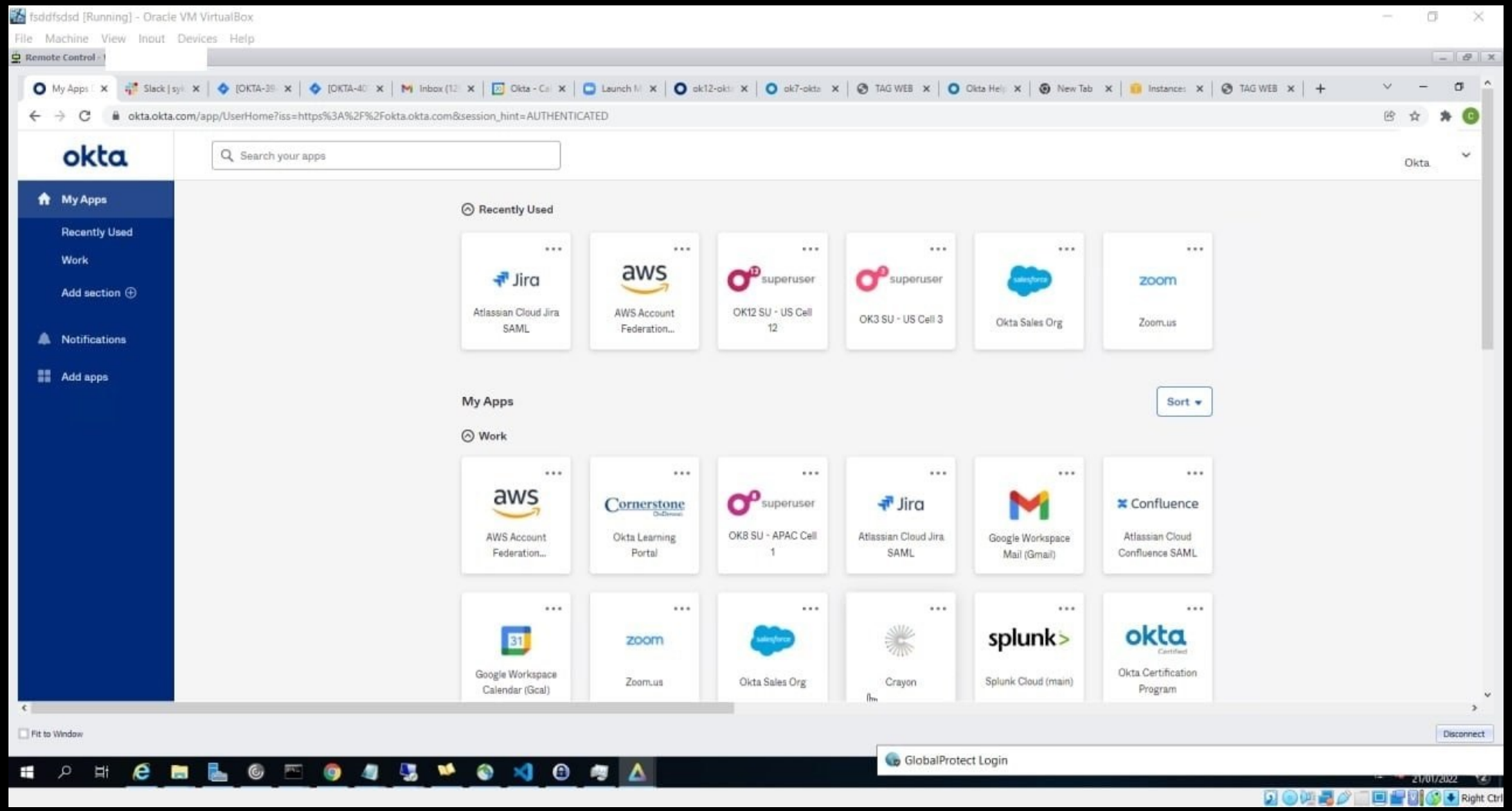
Nošifrētas sistēmas:

- **800 – 1500 uzņēmumos**
- **datorsistēmu skaits varētu būt > 100000**

Log4j (2020)

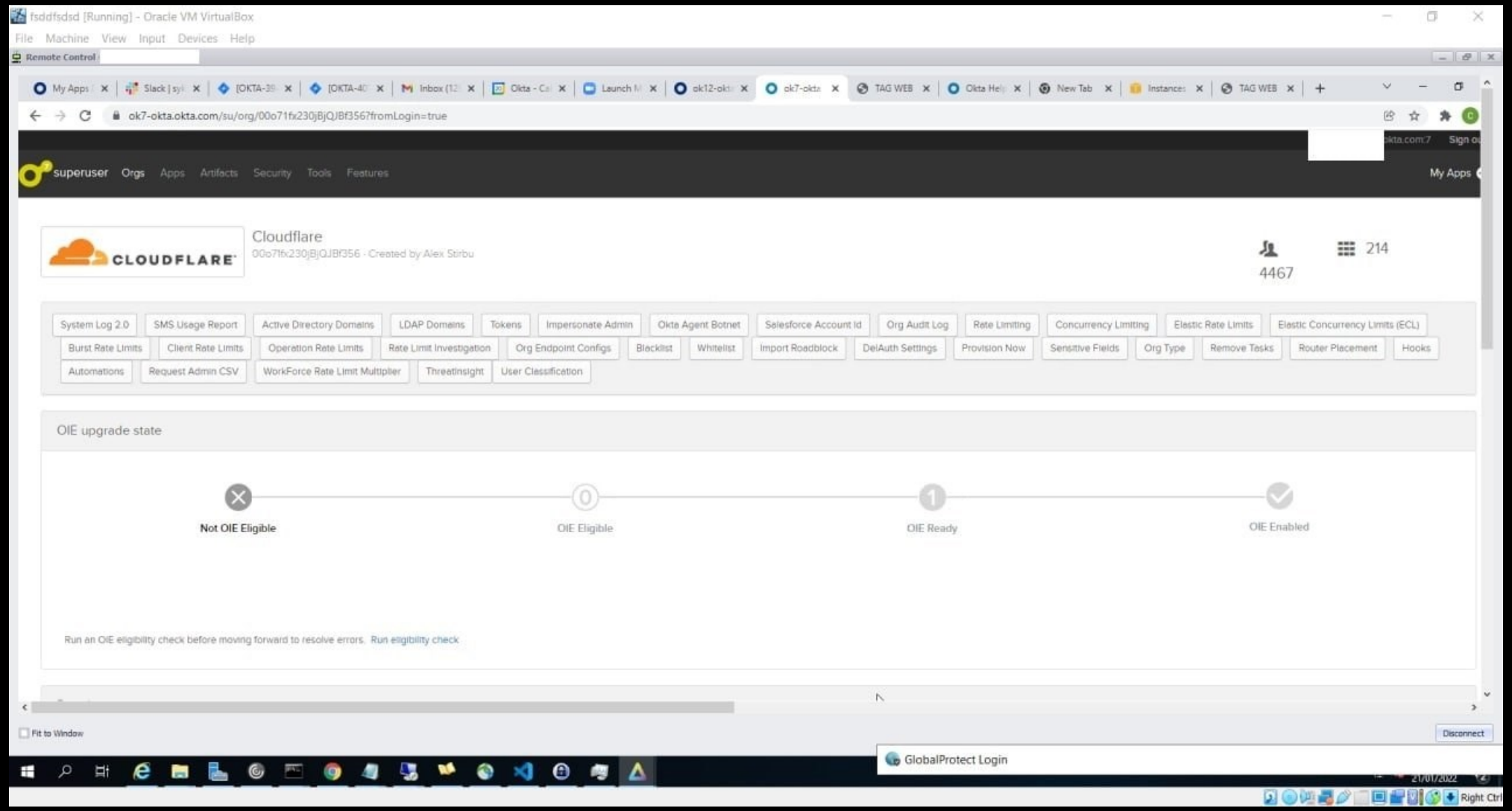
- **Log4j – populāra bibliotēka, de-facto standarts**
- **Ievainojamas visas Log4j 2.x versijas (8 gadu laikā)**
- **Triviāli ekspluatējama «command injection»**

Okta (2022)



https://twitter.com/BillDemirkapi/status/1506107157124722690

Okta (2022)



https://twitter.com/BillDemirkapi/status/1506107157124722690

CloudFlare komentārs

Matthew Prince
@eastdakota

We are aware that @Okta may have been compromised. There is no evidence that Cloudflare has been compromised. Okta is merely an identity provider for Cloudflare. Thankfully, we have multiple layers of security beyond Okta, and would never consider them to be a standalone option.

10:38 PM · Mar 21, 2022 · Echofon

228 Retweets **46** Quote Tweets **1,362** Likes

https://twitter.com/eastdakota/status/1506143353544478724

Software Bill of Materials

Apraksta programmatūrā lietotās komponentes un to versijas

Formāls, mašīnlasāms formāts

Attiecināms arī uz atvērto pirmkodu

ASV: https://www.ntia.gov/sbom

Eiropā un citviet pasaulē šobrīd šādas prasības nav


CERT.LV
Paldies par uzmanību!
certlv
certlv