

Piegādes ķēžu uzbrukumi

Andrejs Konstantinovs

CERT.LV, 24.03.2022



Satura rādītājs

- 1. Kas ir piegādes ķēdes?**
 - 2. Ar piegādes ķēdēm saistītie riski**
 - 3. Zināmie uzbrukumi piegādes ķēdēm**
 - 4. Software bill of materials**
-

Kas ir piegādes ķēdes

amazon
Hello, Sign in Account & Lists Returns & Orders

All Today's Deals Customer Service Registry Gift Cards Sell

1-48 of over 1,000 results for "supply chain management" Sort by: Featured

Kindle Unlimited

Kindle Unlimited Eligible

Department

Books

- Production & Operations
- Business Management
- Engineering
- Business Operations Research
- Business Decision Making
- Office Management
- Accounting

Kindle Store

- Business Management & Leadership

Customer Reviews

★★★★★ & Up

★★★★☆ & Up

★★★☆☆ & Up

★★☆☆☆ & Up

★☆☆☆☆ & Up

Deals & Discounts

All Discounts

New Releases

Last 30 days

Last 90 days

Coming Soon

Book Format

Paperback

Hardcover

Kindle Edition

Large Print

Audible Audiobook

Printed Access Code

Loose Leaf

Audio CD

Author

F. Robert Jacobs

Sumil Chopra


Richard B. Chase

Richard Chase

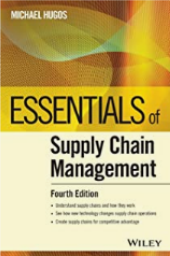
Book Language

English

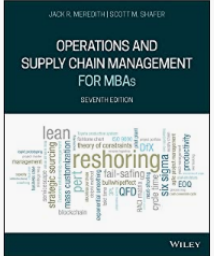
RESULTS



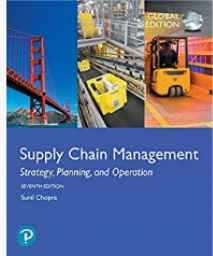
Supply Chain Management For Dummies
by Daniel Stanton
★★★★★ ~ 99
Paperback
\$20²⁹ ~~\$29.99~~
Ships to Latvia
More Buying Choices
\$18.25 (45 used & new offers)
Other formats: Audible Audiobook, Kindle, Audio CD



Essentials of Supply Chain Management (Essentials Series)
Part of: Essentials (16 Books)
★★★★★ ~ 136
Paperback
\$27⁰⁰ to rent
\$28.49 to buy
Ships to Latvia
More Buying Choices
\$19.19 (57 used & new offers)
Other format: Kindle




Operations and Supply Chain Management for MBAs
by Jack R. Meredith and Scott M. Shafer
★★★★★ ~ 55
Paperback
\$66⁹⁰ ~~\$75.95~~
Ships to Latvia
More Buying Choices
\$50.91 (21 used & new offers)
Other format: eTextbook




Supply Chain Management: Strategy, Planning, and Operation, Global Edition
Part of: What's New in Operations Management (5 Books)
★★★★★ ~ 173
Paperback
\$50⁰⁷ ~~\$68.99~~
Ships to Latvia
Only 4 left in stock - order soon.
More Buying Choices
\$49.99 (29 used & new offers)
Other formats: eTextbook, Hardcover


MORE RESULTS



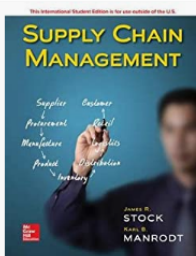
OPERATIONS AND SUPPLY CHAIN MANAGEMENT
ESSENTIALLY YOU ALWAYS WANTED TO KNOW
ASILEY MCCORMICK



THE SUPPLY CHAIN REVOLUTION
INNOVATIVE SOURCING AND LOGISTICS FOR A FIERCELY COMPETITIVE WORLD
SUMAN SARKAR



OPERATIONS AND SUPPLY CHAIN MANAGEMENT
THE CORE
F. ROBERT JACOBS
RICHARD B. CHASE



SUPPLY CHAIN MANAGEMENT
Supplier Customer
Procurement Retail
Manufacture Logistics
Product Distribution
Inventory
JAMES R. STOCK
THOMAS A. MANRODT

- **Programmas (un programmas komponentu) 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

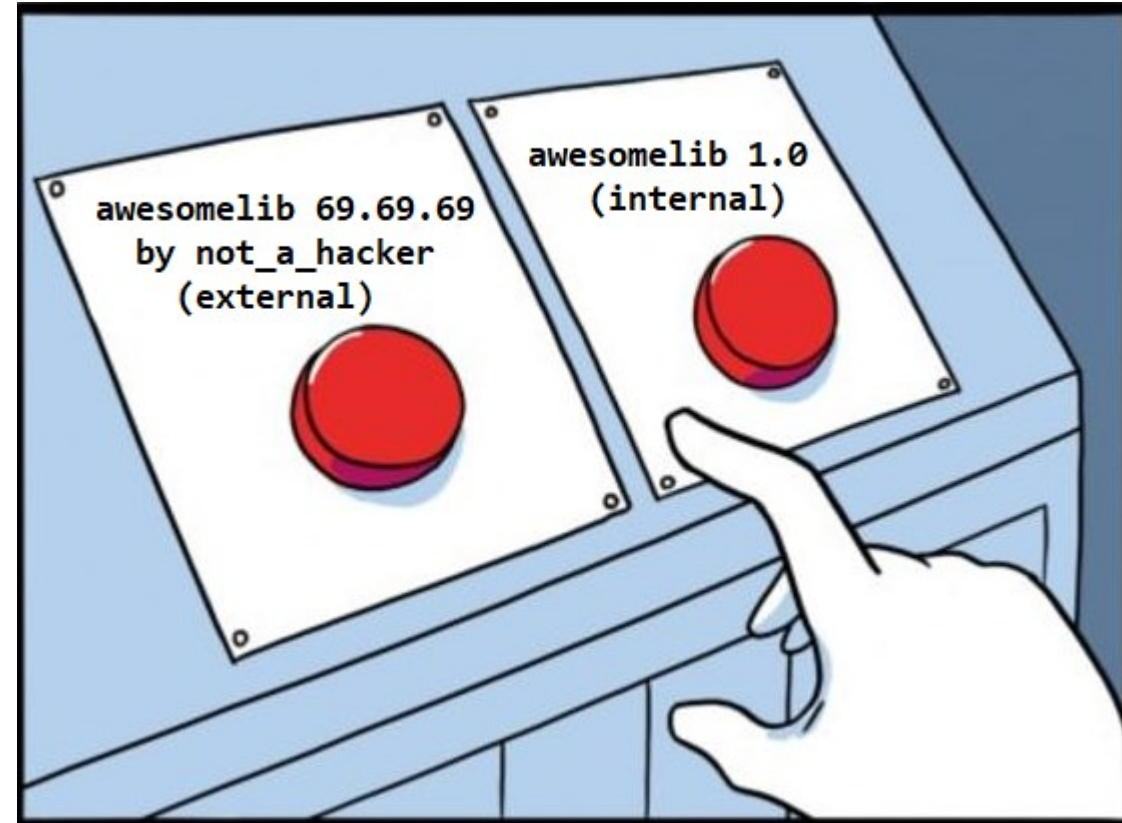
Rezultāts:

- **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 VSA:

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

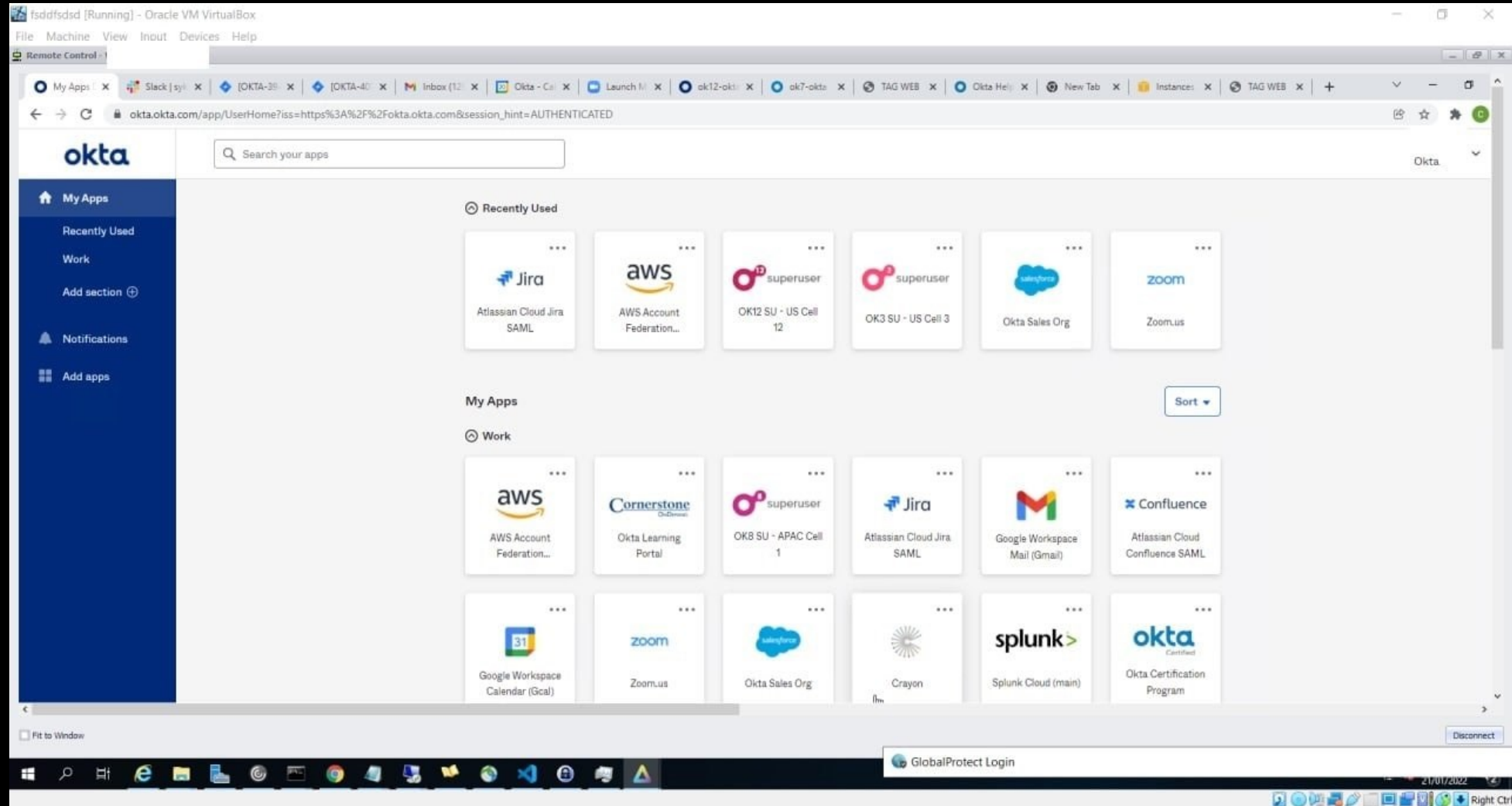
Nošifrētas sistēmas:

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

Log4j (2020)

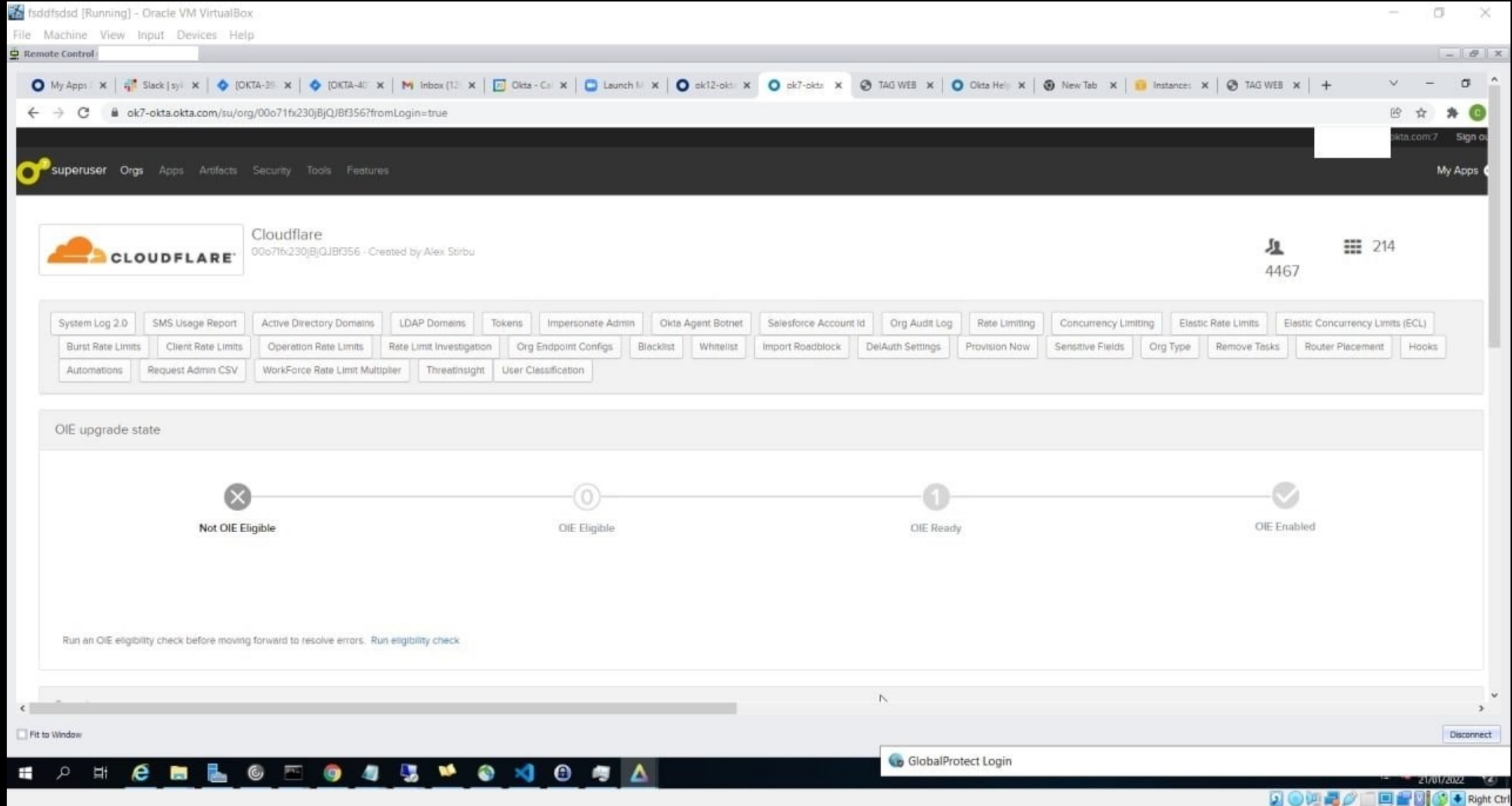
- **Log4j – populāra bibliotēka, de-facto standarts**
 - **ievainojamas visas Log4j 2.x versijas (8 gadu laikā)**
 - **Triviāli ekspluatējama «command injection»**
-

Okta (2022)



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

Okta (2022)



The screenshot shows the Okta admin console interface. At the top, there's a navigation bar with the user 'superuser' and various menu items like 'Orgs', 'Apps', 'Artifacts', 'Security', 'Tools', and 'Features'. Below this, the main content area displays the 'Cloudflare' organization details, including the ID '00o71fx230j8jQJBF356' and the creator 'Alex Sirbu'. A grid of various configuration buttons is visible, such as 'System Log 2.0', 'SMS Usage Report', 'Active Directory Domains', 'LDAP Domains', 'Tokens', 'Impersonate Admin', 'Okta Agent Botnet', 'Salesforce Account Id', 'Org Audit Log', 'Rate Limiting', 'Concurrency Limiting', 'Elastic Rate Limits', 'Elastic Concurrency Limits (ECL)', 'Burst Rate Limits', 'Client Rate Limits', 'Operation Rate Limits', 'Rate Limit Investigation', 'Org Endpoint Configs', 'Blacklist', 'Whitelist', 'Import Roadblock', 'DelAuth Settings', 'Provision Now', 'Sensitive Fields', 'Org Type', 'Remove Tasks', 'Router Placement', 'Hooks', 'Automations', 'Request Admin CSV', 'WorkForce Rate Limit Multiplier', 'Threatinsight', and 'User Classification'. The central focus is the 'OIE upgrade state' section, which features a progress bar with four stages: 'Not OIE Eligible' (marked with an 'X'), 'OIE Eligible' (marked with '0'), 'OIE Ready' (marked with '1'), and 'OIE Enabled' (marked with a checkmark). Below the progress bar, a note reads: 'Run an OIE eligibility check before moving forward to resolve errors. Run eligibility check'. The bottom of the screenshot shows the Windows taskbar with various application icons and a 'GlobalProtect Login' notification.

<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



Paldies par
uzmanību!