Omówienie przykładu wycieku danych

Case study



Mateusz Kopacz
Chief Security Architect

integrity partners

W Polsce kwestię kradzieży tożsamości i nękania reguluje Art. 190a. Kodeksu Karnego.

§ 1.

Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2.

Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej.

§ 3.

Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 12.

§ 4.

Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Ofiary oszustwa mogą zgłosić to przestępstwo na policję w miejscu zamieszkania lub do prokuratury.

Psychologiczne aspekty które wykorzystują przestępcy / oszuści / scamerzy

- „Wywieranie wpływu na ludzi (teoria i praktyka)”
- 15 lat badań
- przetłumaczona na 26 języków
- sprzedana w ponad 3 mln egzemplarzy



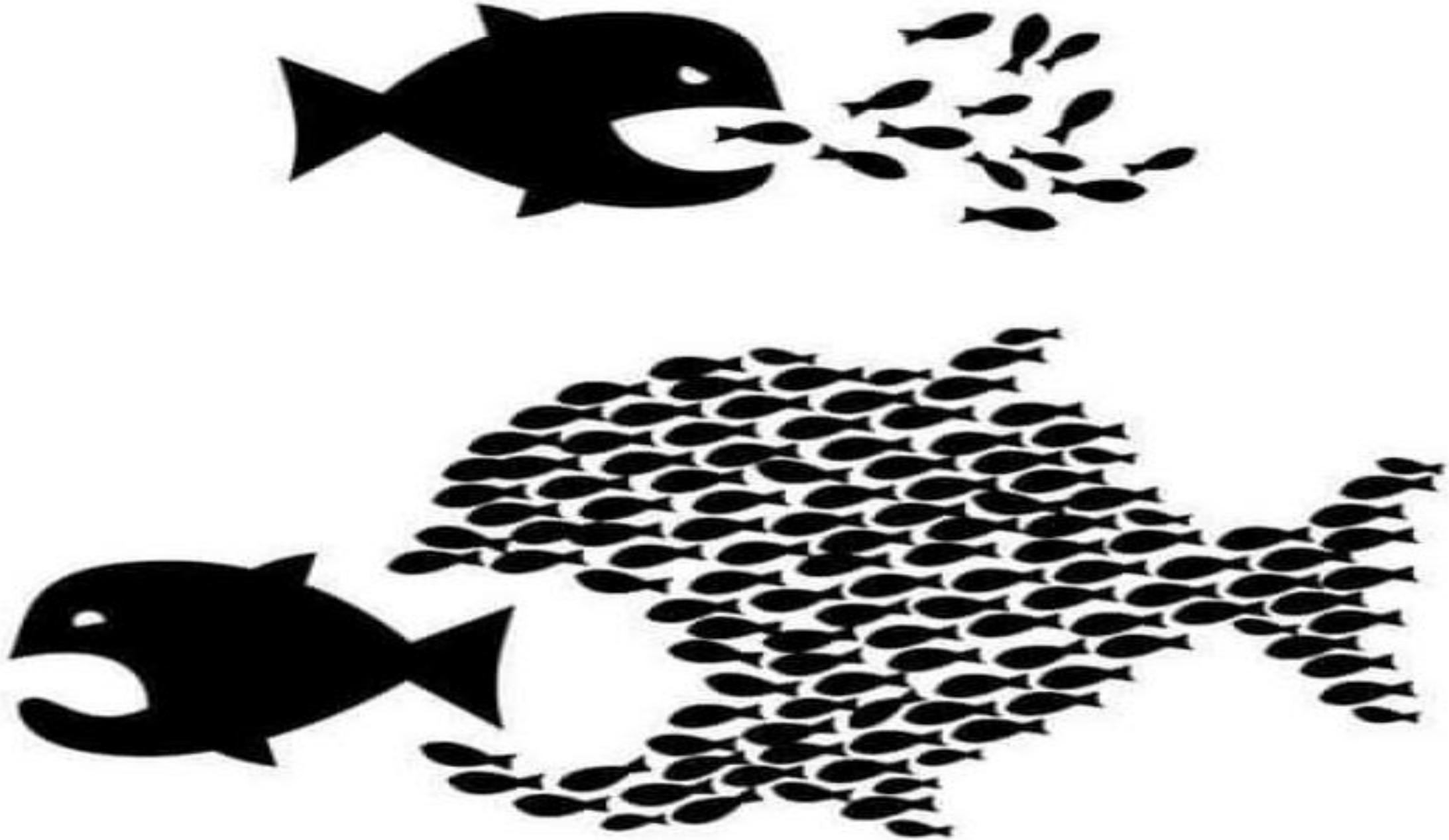
Dr Robert Cialdini

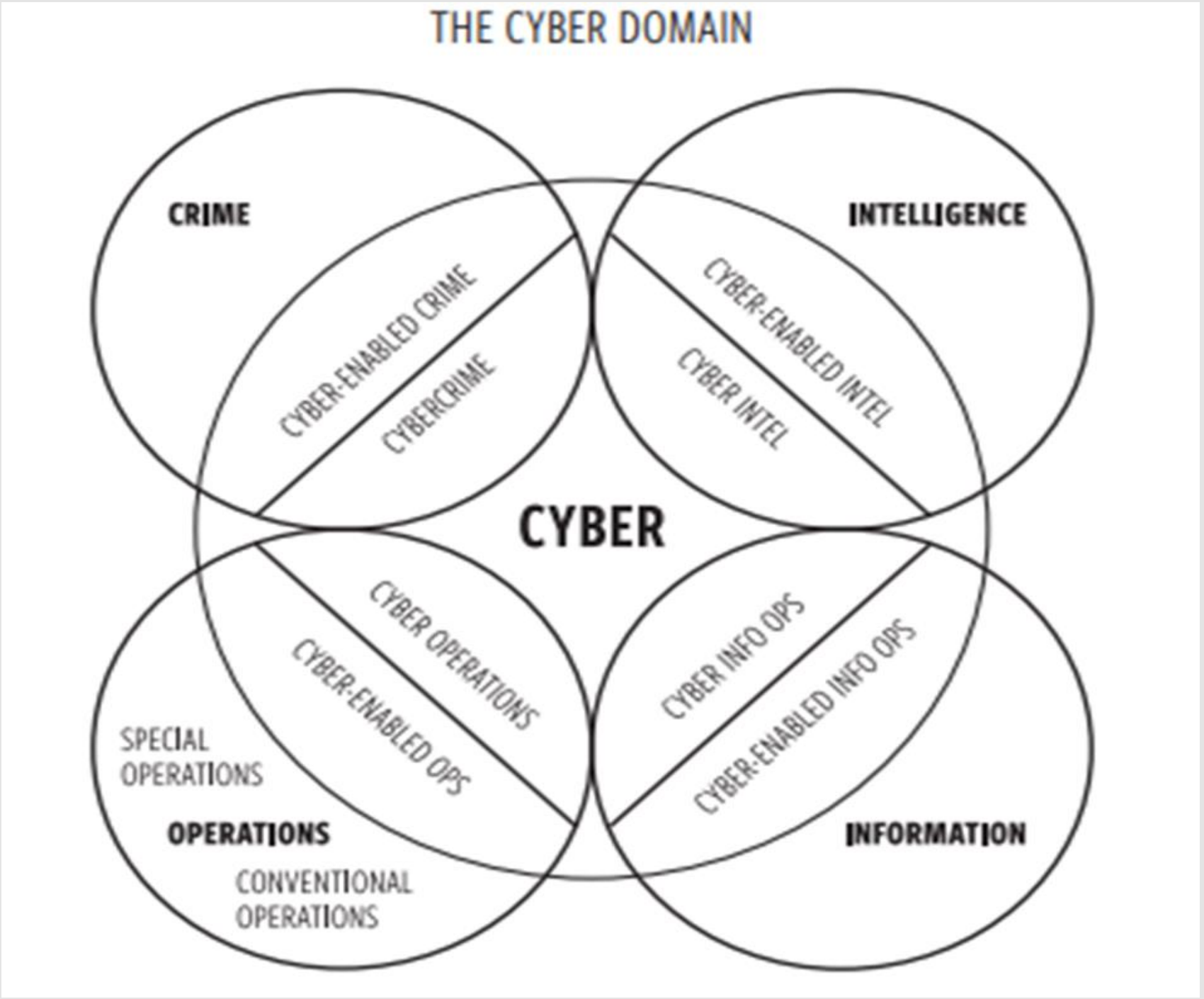
Robert Beno Cialdini (ur. 27 kwietnia 1945) – profesor psychologii Uniwersytetu Stanowego w Arizonie

Jako pierwszy sklasyfikował metody stosowane do wywierania wpływu na ludzi w postaci 6 „zasad”

1. **Zasada wzajemności**
2. **Zasada zobowiązanie i konsekwencja**
3. **Dowód społeczny** („inni tak robią”)
4. **Lubienie kogoś** (przeniesienie uczuć dotyczących osoby na przekazywaną przez nią propozycję)
5. **Autorytet** (oceniamy go według atrybutów, a nie merytorycznej wartości przekazu)
6. **Niedobór czegoś** („może zabraknąć”)






THE CYBER DOMAIN
CRIME
INTELLIGENCE
CYBER-ENABLED CRIME
CYBERCRIME
CYBER-ENABLED INTEL
CYBER INTEL
CYBER
CYBER OPERATIONS
CYBER-ENABLED OPS
CYBER INFO OPS
CYBER-ENABLED INFO OPS
SPECIAL OPERATIONS
OPERATIONS
CONVENTIONAL OPERATIONS
INFORMATION

Modelowanie zagrożeń
(Threat Modeling / Threat Assessment)

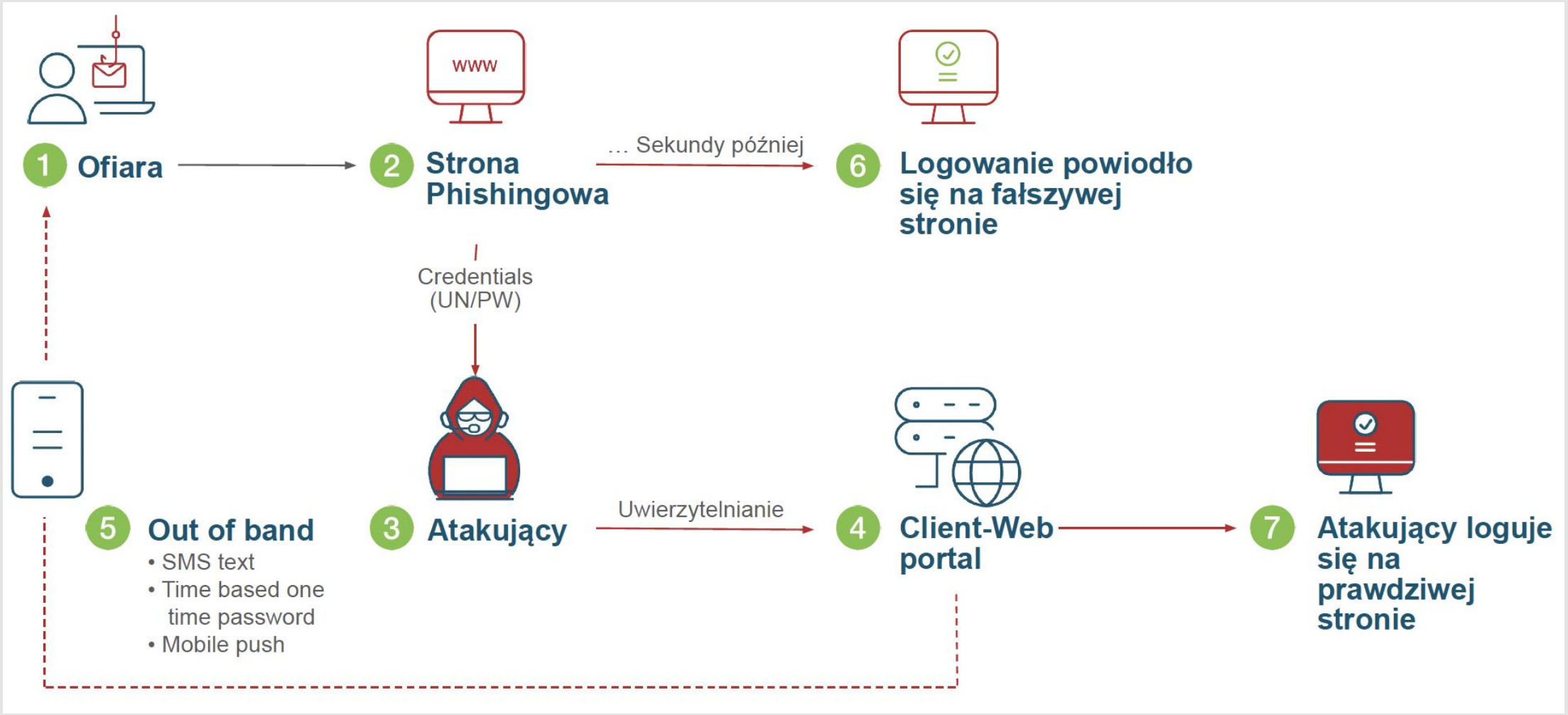
- Modelowanie zagrożeń wykonujemy jeszcze przed budową systemu / aplikacji / serwerowni, aby zdać sobie sprawę z zagrożeń jakie musimy brać pod uwagę.

- To działanie ma pomóc w uniknięciu potencjalnych podatności zarówno architektonicznych jak i implementacyjnych.

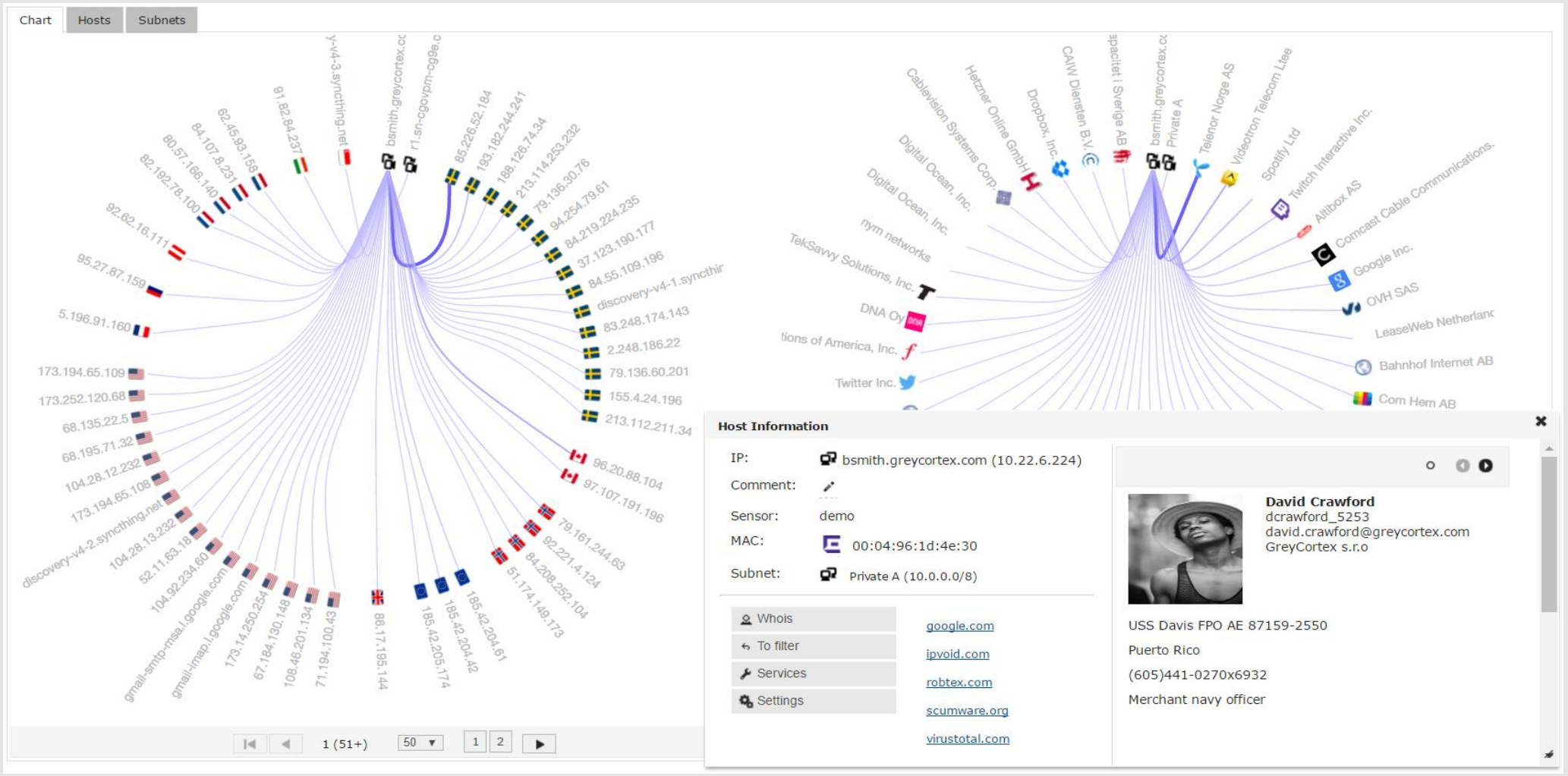
- Dodatkowo wynikowy model zagrożeń możesz wykorzystać do weryfikacji założeń w późniejszych etapach.

Jako eksperci twórzmy bezpieczeństwo aby użytkownik mógł je na co dzień eksploatować a nie mozolnie zabezpieczać i łatać.

Jak strona phishingowa obchodzi tradycyjne MFA?

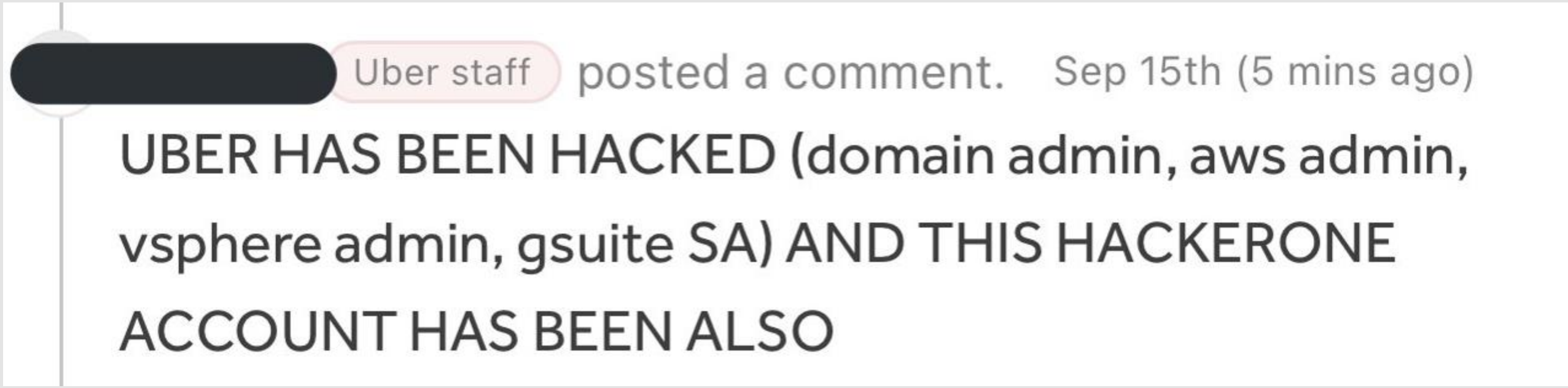


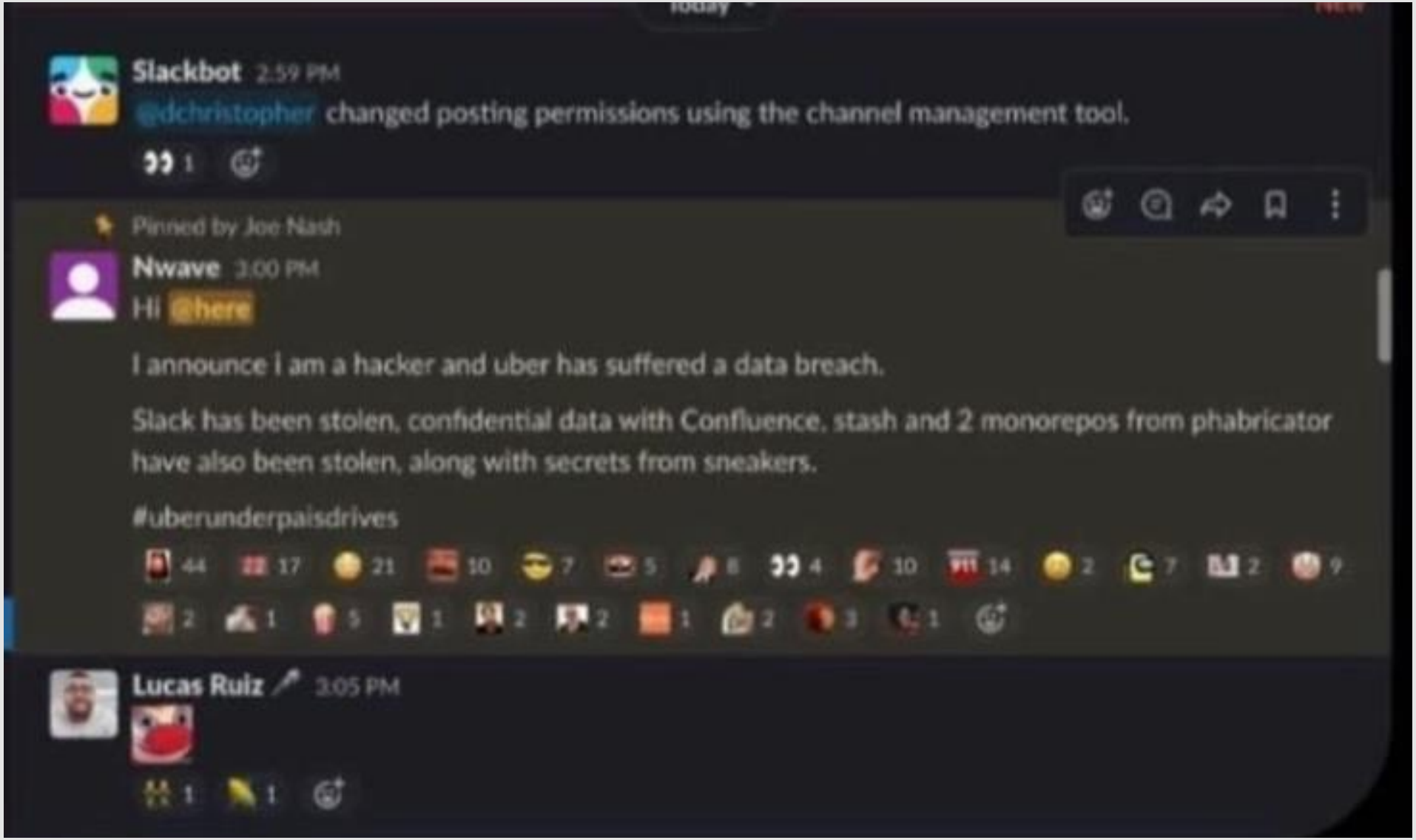
Jak strona phishingowa wykorzystuje SSO?

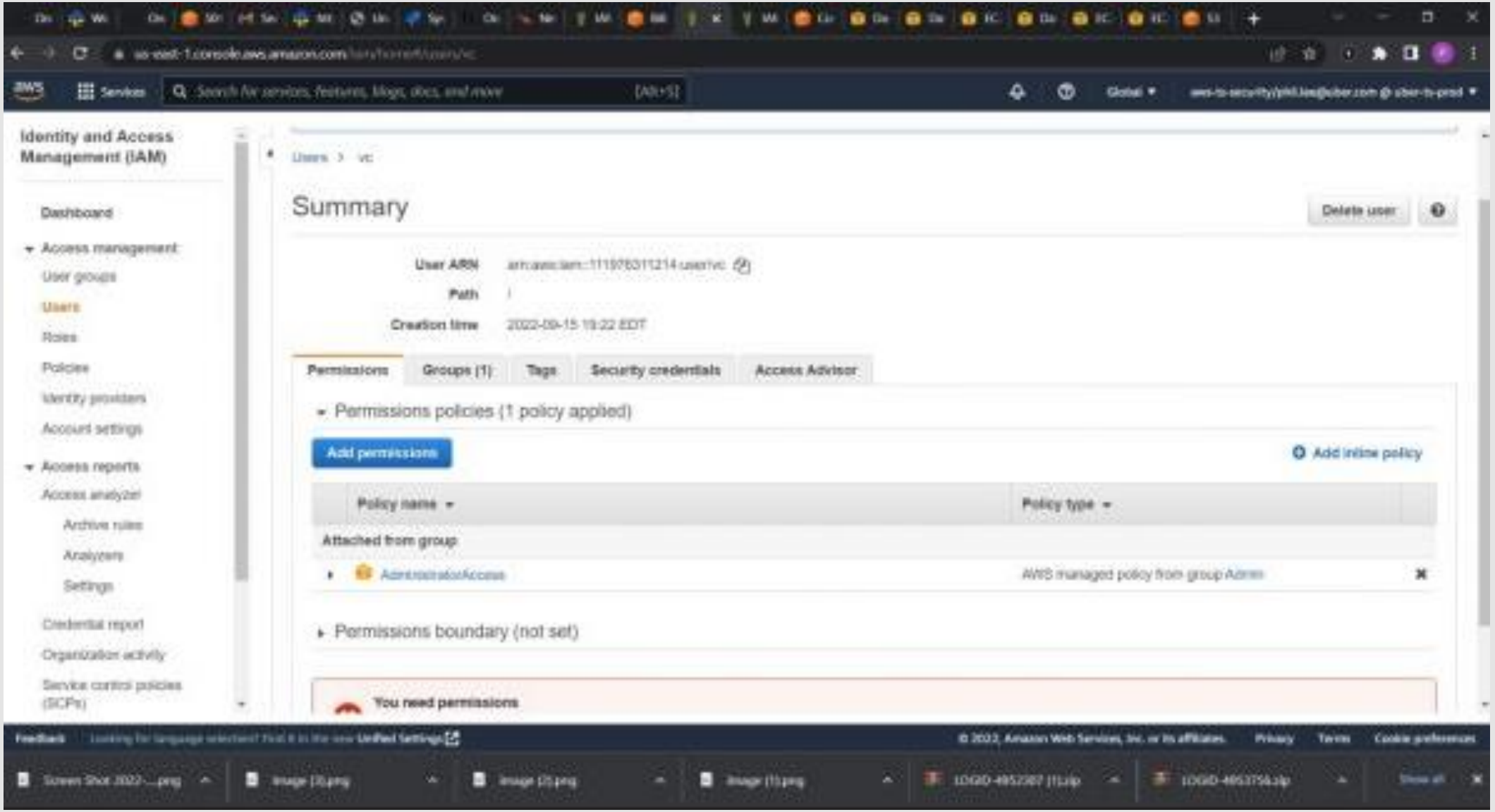


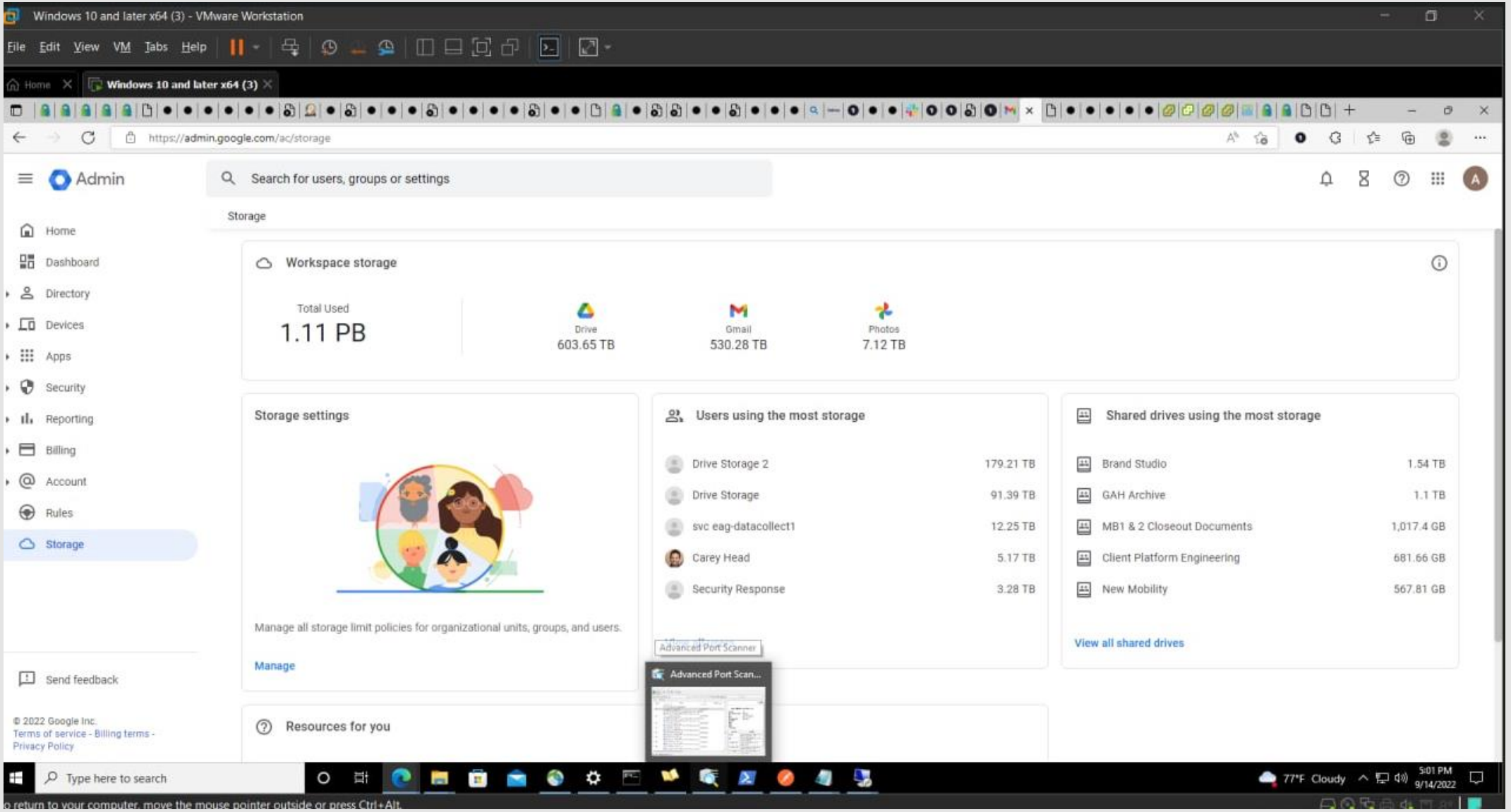
ANATOMIA ATAKU

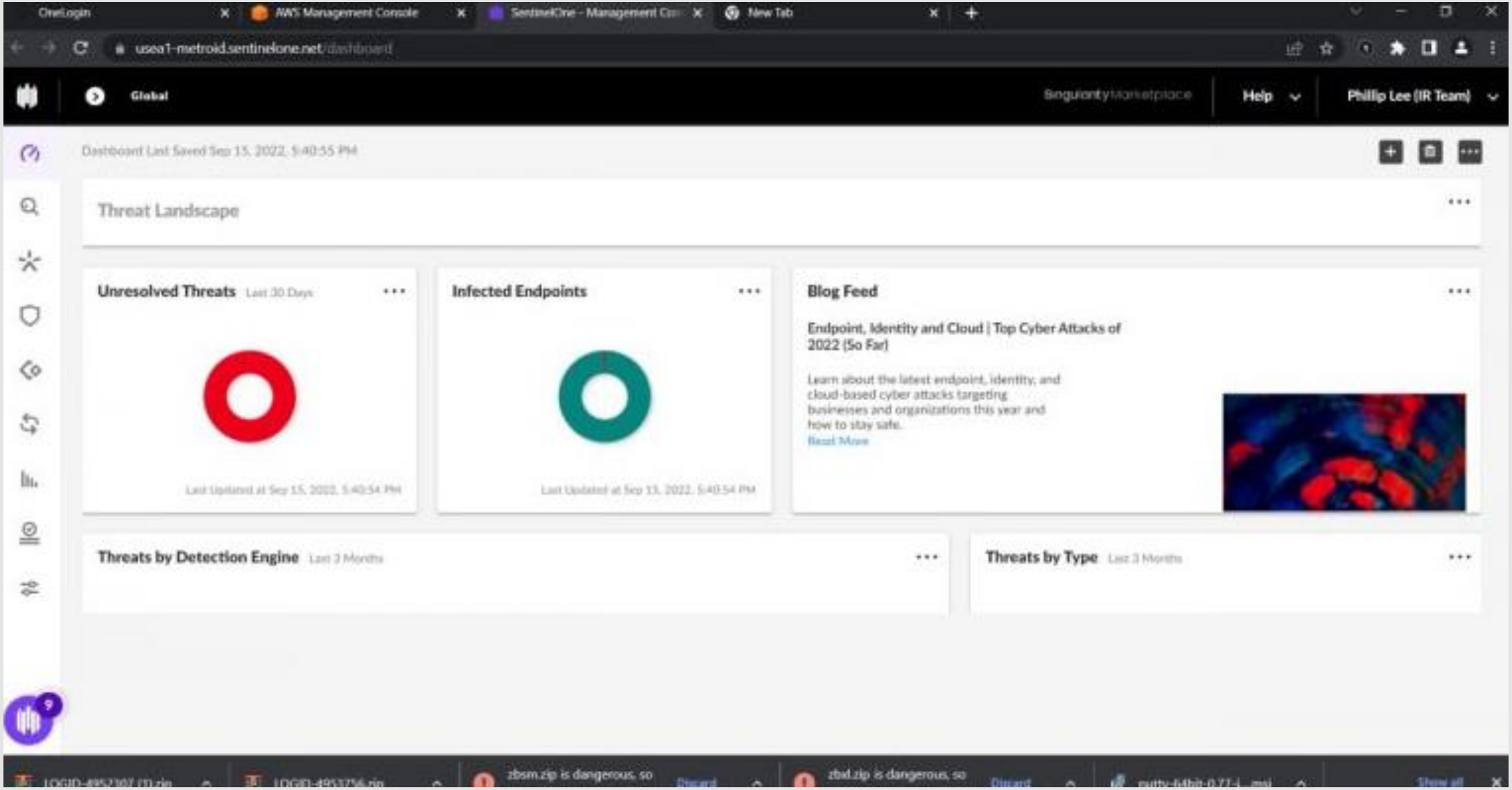


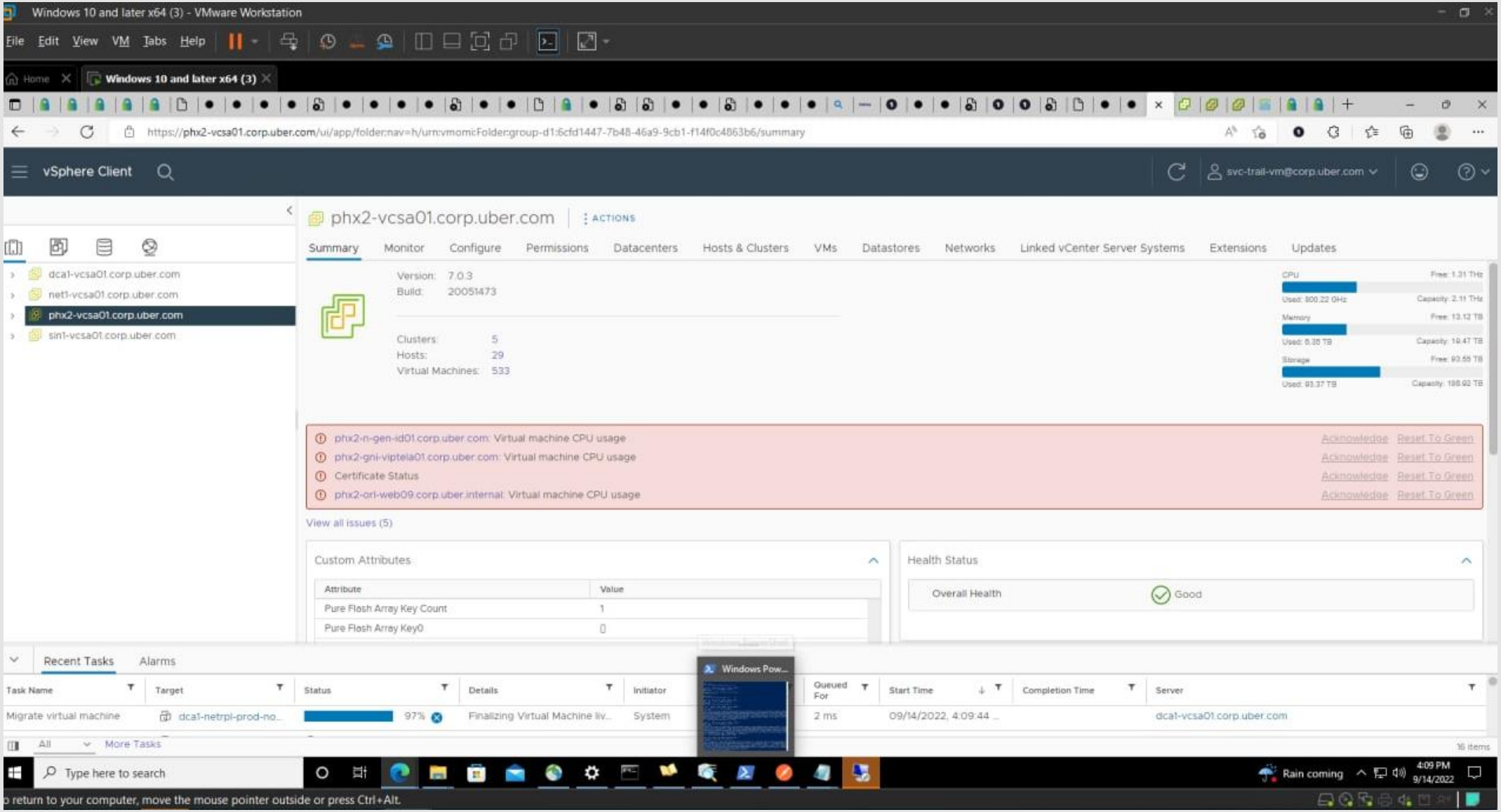

[redacted] Uber staff posted a comment. Sep 15th (5 mins ago)
UBER HAS BEEN HACKED (domain admin, aws admin, vsphere admin, gsuite SA) AND THIS HACKERONE ACCOUNT HAS BEEN ALSO

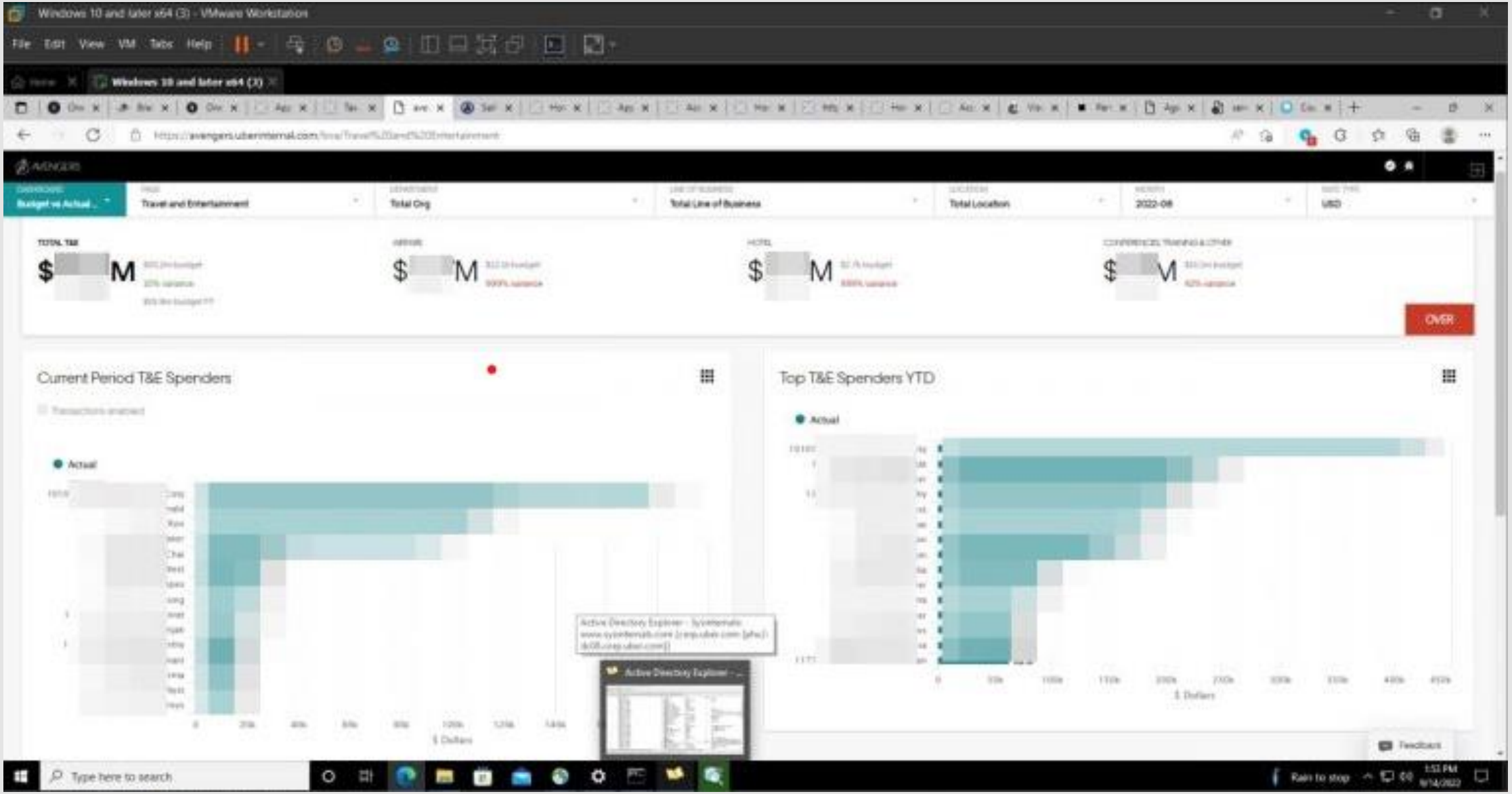

Slackbot 2:59 PM
@dchristopher changed posting permissions using the channel management tool.
Pinned by Joe Nash
Nwave 3:00 PM
Hi @here
I announce I am a hacker and uber has suffered a data breach.
Slack has been stolen, confidential data with Confluence, stash and 2 monorepos from phabricator have also been stolen, along with secrets from sneakers.
#uberunderpaisdrives
Lucas Ruiz 3:05 PM


Identity and Access Management (IAM)
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Summary
Delete user
User ARN
Path
Creation time
2022-09-15 19:22 EDT
Permissions
Groups (1)
Tags
Security credentials
Access Advisor
Permissions policies (1 policy applied)
Add permissions
Add inline policy
Policy name
Policy type
Attached from group
AdministratorAccess
AWS managed policy from group Admin
Permissions boundary (not set)
You need permissions


Windows 10 and later x64 (3) - VMware Workstation
File Edit View VM Tabs Help
Windows 10 and later x64 (3)
https://admin.google.com/ac/storage
Admin
Search for users, groups or settings
Storage
Home
Dashboard
Directory
Devices
Apps
Security
Reporting
Billing
Account
Rules
Storage
Send feedback
© 2022 Google Inc.
Terms of service - Billing terms -
Privacy Policy
Workspace storage
Total Used
1.11 PB
Drive
603.65 TB
Gmail
530.28 TB
Photos
7.12 TB
Storage settings
Manage all storage limit policies for organizational units, groups, and users.
Manage
Users using the most storage
Drive Storage 2 179.21 TB
Drive Storage 91.39 TB
svc eag-datacollect1 12.25 TB
Carey Head 5.17 TB
Security Response 3.28 TB
Shared drives using the most storage
Brand Studio 1.54 TB
GAH Archive 1.1 TB
MB1 & 2 Closeout Documents 1,017.4 GB
Client Platform Engineering 681.66 GB
New Mobility 567.81 GB
View all shared drives
Advanced Port Scanner
Advanced Port Scan...
Resources for you
Type here to search
77°F Cloudy
5:01 PM
9/14/2022


OneLogin
AWS Management Console
SentinelOne - Management Con
New Tab
usea1-netroid.sentinelone.net/dashboard
Global
Singularity Marketplace
Help
Phillip Lee (IR Team)
Dashboard Last Saved Sep 15, 2022, 5:40:55 PM
Threat Landscape
Unresolved Threats
Last 30 Days
Last Updated at Sep 15, 2022, 5:40:54 PM
Infected Endpoints
Last Updated at Sep 15, 2022, 5:40:54 PM
Blog Feed
Endpoint, Identity and Cloud | Top Cyber Attacks of 2022 (So Far)
Learn about the latest endpoint, identity, and cloud-based cyber attacks targeting businesses and organizations this year and how to stay safe.
Read More
Threats by Detection Engine
Last 3 Months
Threats by Type
Last 3 Months
zbsm.zip is dangerous, so
Discard
zbd.zip is dangerous, so
Discard
Show all


Windows 10 and later x64 (3) - VMware Workstation
File Edit View VM Tabs Help
Home
Windows 10 and later x64 (3)
https://phx2-vcsa01.corp.uber.com/ui/app/folder;nav=h/urn:vmomi:Folder:group-d1:6cfd1447-7b48-46a9-9cb1-f14f0c4863b6/summary
vSphere Client
svc-trail-vm@corp.uber.com
phx2-vcsa01.corp.uber.com
ACTIONS
Summary Monitor Configure Permissions Datacenters Hosts & Clusters VMs Datastores Networks Linked vCenter Server Systems Extensions Updates
dca1-vcsa01.corp.uber.com
net1-vcsa01.corp.uber.com
phx2-vcsa01.corp.uber.com
sin1-vcsa01.corp.uber.com
Version: 7.0.3
Build: 20051473
Clusters: 5
Hosts: 29
Virtual Machines: 533
phx2-n-gen-id01.corp.uber.com: Virtual machine CPU usage
phx2-gni-viptela01.corp.uber.com: Virtual machine CPU usage
Certificate Status
phx2-ori-web09.corp.uber.internal: Virtual machine CPU usage
Acknowledge Reset To Green
View all issues (5)
Custom Attributes
Attribute Value
Pure Flash Array Key Count 1
Pure Flash Array Key0 0
Health Status
Overall Health Good
Recent Tasks Alarms
Task Name Target Status Details Initiator Queued For Start Time Completion Time Server
Migrate virtual machine dca1-netrpl-prod-no... 97% Finalizing Virtual Machine liv... System 2 ms 09/14/2022, 4:09:44 ... dca1-vcsa01.corp.uber.com
All More Tasks
Windows Pow...
Type here to search
Rain coming
4:09 PM 9/14/2022
o return to your computer, move the mouse pointer outside or press Ctrl+Alt.


Windows 10 and later x64 (3) - VMware Workstation
File Edit View VM Tabs Help
Travel and Entertainment
Total Org
Total Line of Business
Total Location
2022-08
USD
OVER
Current Period T&E Spenders
Actual
Top T&E Spenders YTD
Actual
Type here to search

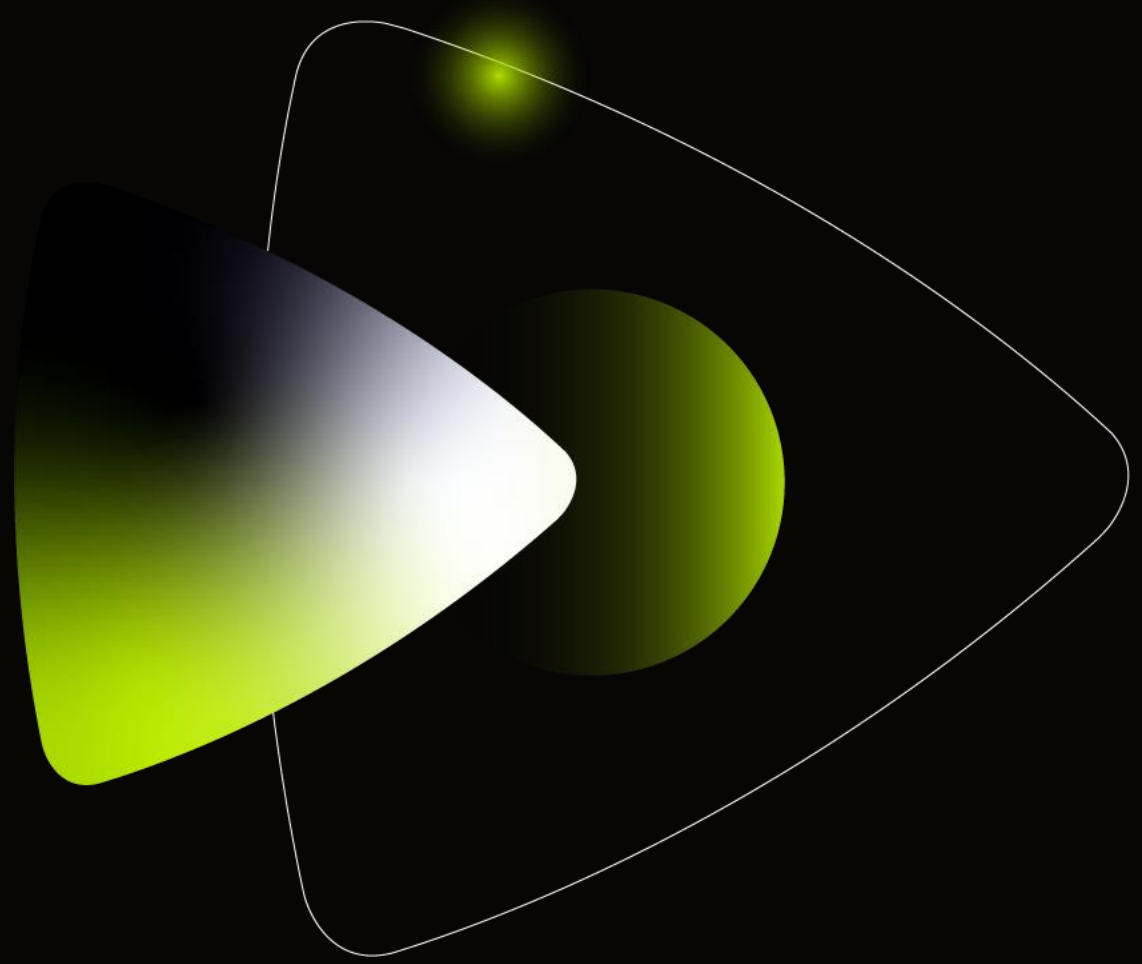

Tea Pot
last seen just now
ok so basically uber had a network share \\ ots. the share contained some powershell scripts.
one of the powershell scripts contained the username and password for a admin user in Thycotic (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, GSuite
8:05 PM
on an uber IP range? or v on like GCP or AWS (*.uberinternal)
edited 8:06 PM
in Uber intranet 8:07 PM
*.corp.uber.com edited 8:07 PM
How'd you get access to the intranet then? 8:08 PM
SE an employee -> access VPN -> scan intranet? 8:08 PM
yes! 8:08 PM
exactly 8:08 PM

Dziękuję za uwagę!

Mateusz Kopacz

604 754 160

mateusz.kopacz@integritypartners.pl



integrity partners