North America Community Meeting 2023

PCI Security Standards Council

PCI Security Standards Council

North America

Community Meeting 2023

PCI Security Standards Council

Cloudy With a Chance of Breaches

Where CHD May Be Hiding and at Risk

CONVERGE TECHNOLOGY SOLUTIONS

ACCUDATA SYSTEMS A CONVERGE COMPANY

Presented by:
Anton Abaya, CISM, CISA, PCI QSA
Professional Services Manager - Governance, Risk, and Compliance

Agenda

- Introduction
- Rapid Cloud Growth & Security Challenges
- Case Studies: Real-World Cloud Cardholder Data Environments
- Key Takeaways

PCI Security Standards Council

About Me

Anton Abaya

- **WILDLY PASSIONATE** in All Cybersecurity and PCI DSS
- Professional Services Manager of GRC Team, vCISO, and Cloud Security
- Principal Consultant
  - PCI QSA: 15+ years
  - Penetration Tester / Red Teamer / Social Engineer
  - Developed Our Cloud Security Assessment Methodology

PCI Security Standards Council

About Converge Technology Solutions

60+
Locations
Serving North America & Europe

>4,000
Clients

700+
Vendor Partnerships

30+ Years of Cybersecurity Experience

NOW

200+
Cybersecurity Resources

4,000+
Professional Service Engagements

>10,900
Threat Hunts

70,000
Security Alerts Investigated

2023 YTD

89
Cybersecurity NPS Score

PCI Security Standards Council

Cloud Growth & Security Concerns

FORTUNE BUSINESS INSIGHTS

Cloud Security Market Size to Reach USD 106.02 Billion [2022-2029] | 18.1% CAGR

According to Fortune Business Insights, the global Cloud Security Market Size is projected to hit USD 106.02 Billion in 2029, at CAGR of 18.1 % during forecast period [2022-2026]; Rising Adoption of Cloud Computing Solutions & Applications to Augment Market Growth

Source: Global News Wire

Source: Prasa

PCI Security Standards Council

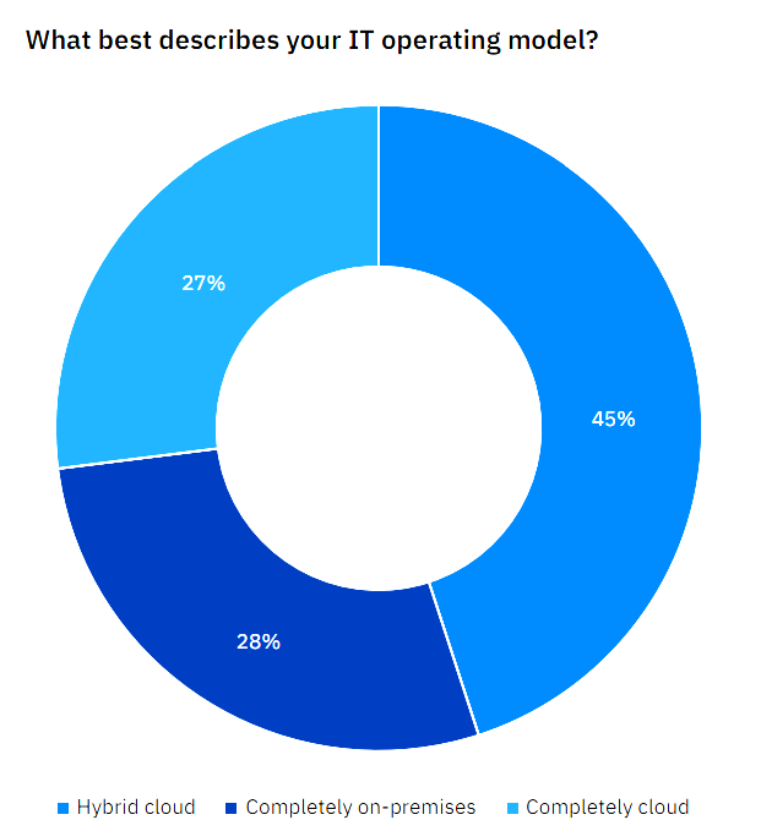
Breaches in the Cloud

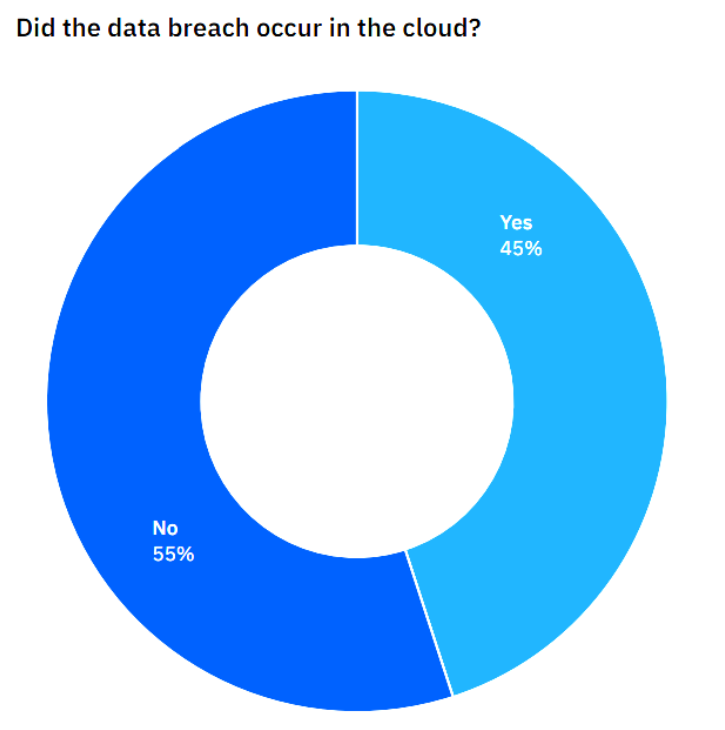
45%

Share of breaches that occurred in the cloud

43%

Share of organizations that were in early stages or had not started applying security practices to safeguard their cloud environments



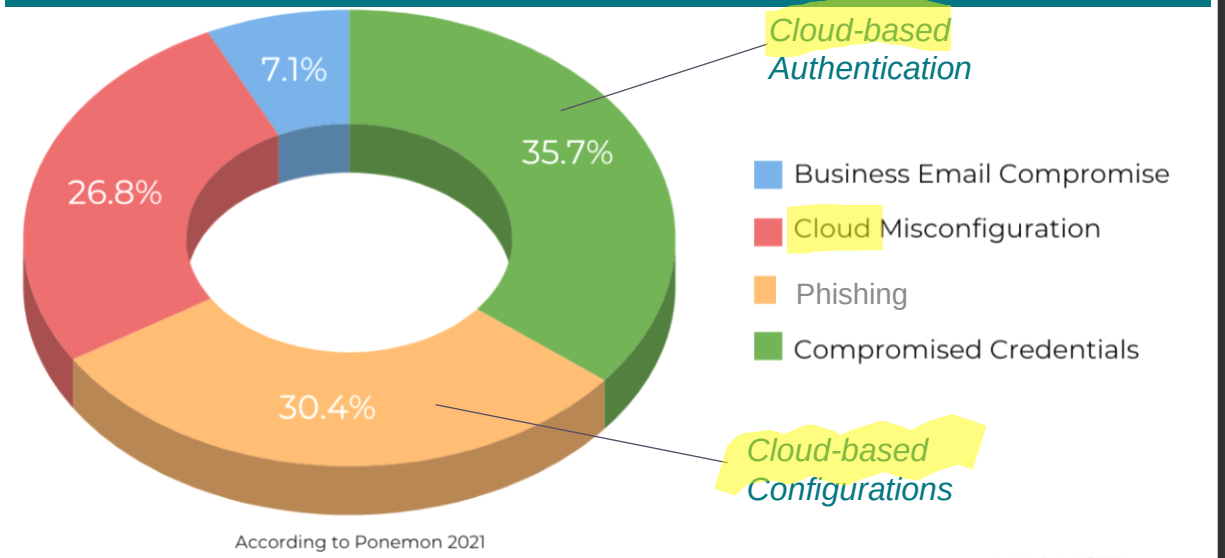


PCI Security Standards Council

Source: IBM Cost of a Data Breach Report 2022

Breaches in the Cloud

Initial Attack Vectors for a Data Breach



According to Ponemon 2021

ustadatastorage.com | 706. 793. 0186

AUGUSTA DATA STORAGE

More Data Points on Data Breaches

45% of Breaches Were Cloud-Based

Nearly half of all breaches occurred in the cloud – and those that occurred in the public cloud were costlier. While hybrid cloud environment breaches cost an average of $3.8M, the average cost in private clouds was $4.24M and in public clouds it was $5.02M!

The Crazy Cost of a Data Breach

A data breach is an expensive matter. Per IBM, the average costs of breaches by type are:

- $4.35M - The average total cost of a data breach
- $4.82M - The average cost of a critical infrastructure data breach. Critical infrastructure includes financial services, industrial technology, energy, transportation, communication, healthcare, education and public sector

PCI Security Standards Council

Source: AugustaDataStorage

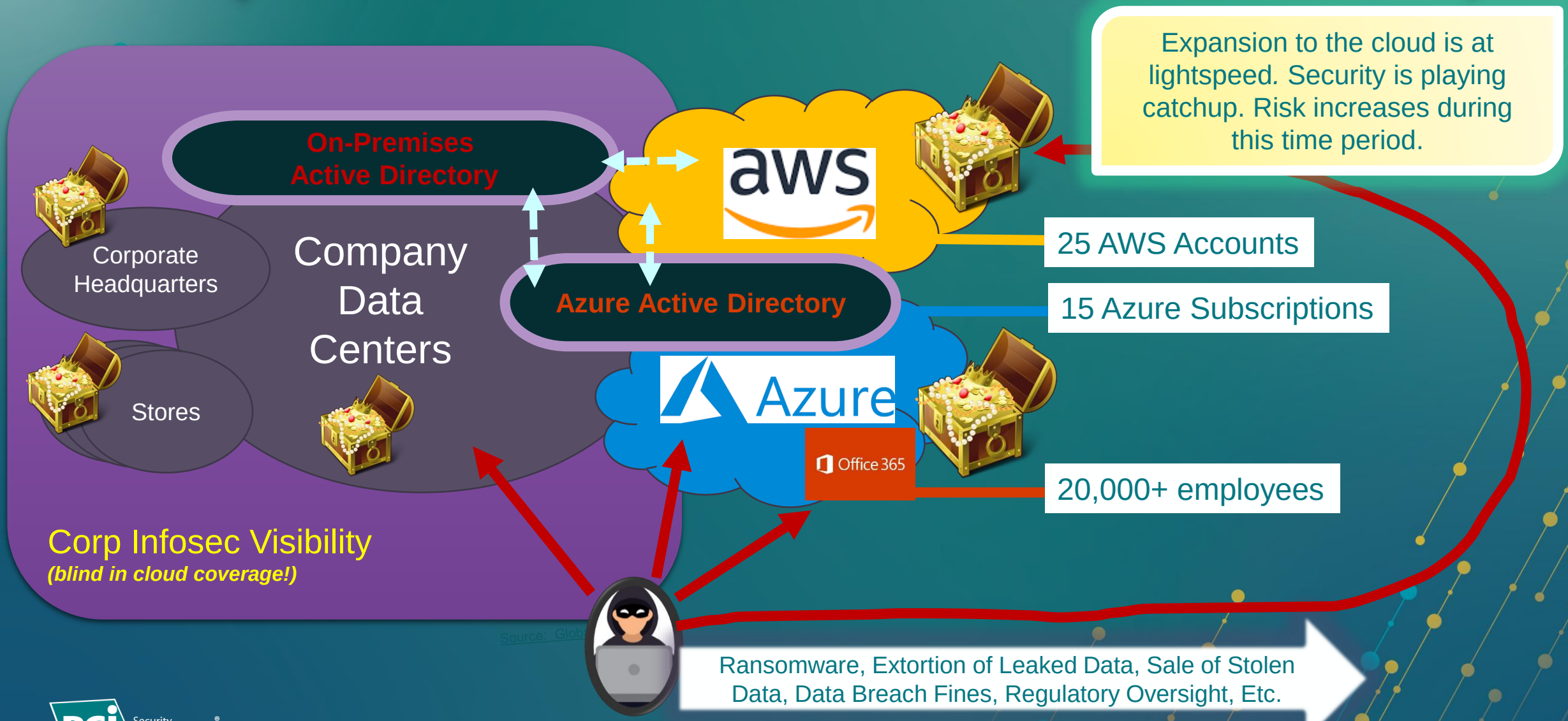
Everything as a Service

- Shadow IT Developers
- Company Acquisitions With Cloud Presence
- Cloud Migrations
- Cloud-First Strategy (New Implementations)
- Move Fast or Lose to Competition

Source: Global News Wi

PCI Security Standards Council

Example: Real-World Cloud Attack Landscape

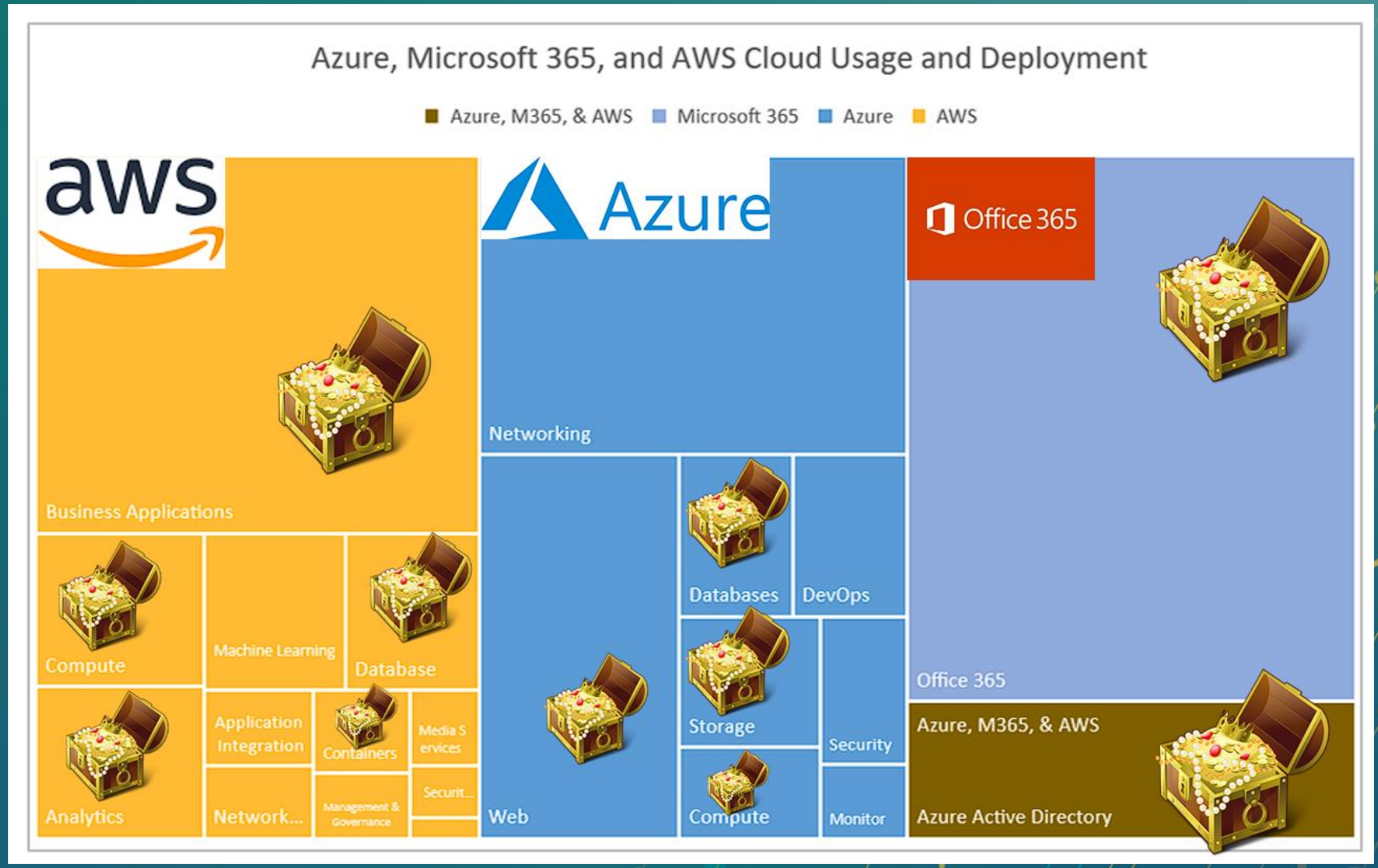


PCI Security Standards Council

Example: Real-World Cloud Attack Landscape

There are unique attack vectors for EACH of these.

Security issues
(cloud control plane misconfigurations)
found affecting all these areas.

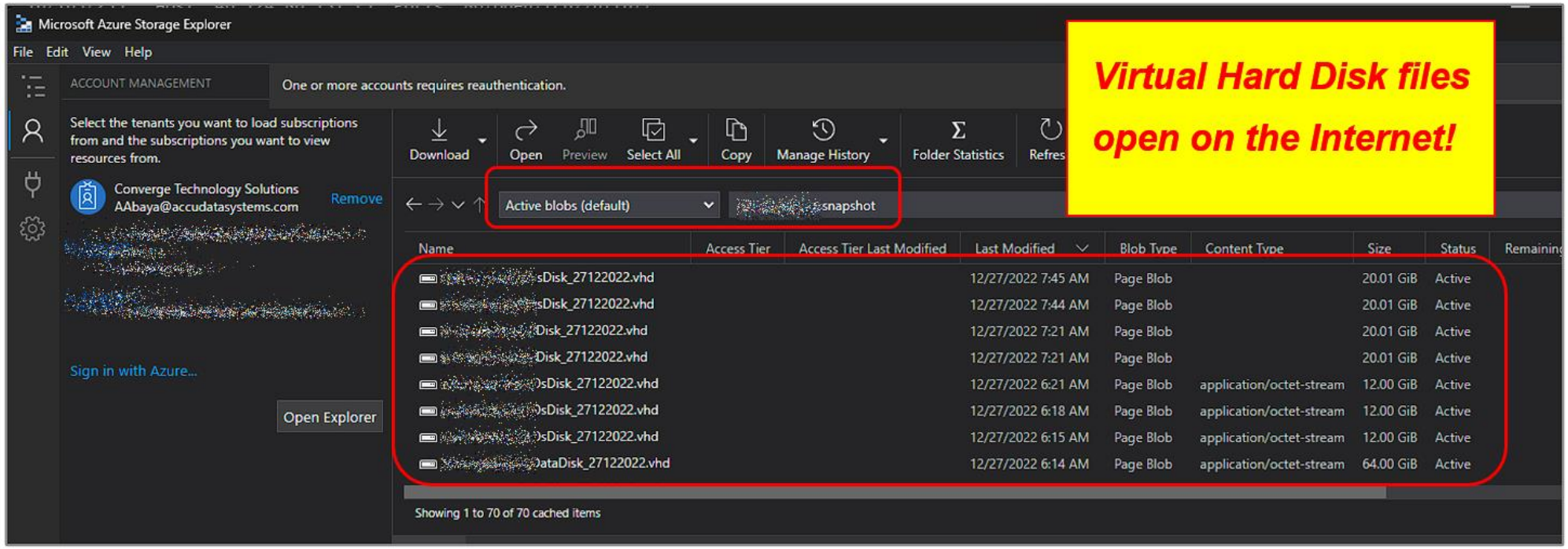


PCI Security Standards Council

Real-World Examples

PUBLIC internet exposure of cloud storage account. **(DATA BREACH)**

Using Azure Storage Explorer, the Blob container was confirmed to be accessible anonymously on the internet. Within this Blob were numerous Virtual Hard Disk (.vhd) files that are presumed to contain **sensitive information**.



PCI Security Standards Council

Real-World Examples

Identity access management (IAM) issues in the cloud.

(DATA BREACH)

Password: 'Company123'

Total [redacted] Accounts:	**17,575**
Total [redacted] *Active* Accounts:	**13,649**
[redacted] *Member* Accounts:	13,364
[redacted] *Guest* Accounts:	285
Total [redacted] *Disabled* Accounts:	**3,926**

157 Privileged Accounts (Azure/AWS)

36 are stale/unused

86 are 'everyday' accounts

1,173 are stale/unused (password change >90 days)
-50% of these have password change >120 days

206 non-person (service/application) accounts

2,584 accounts are *not* required to use MFA

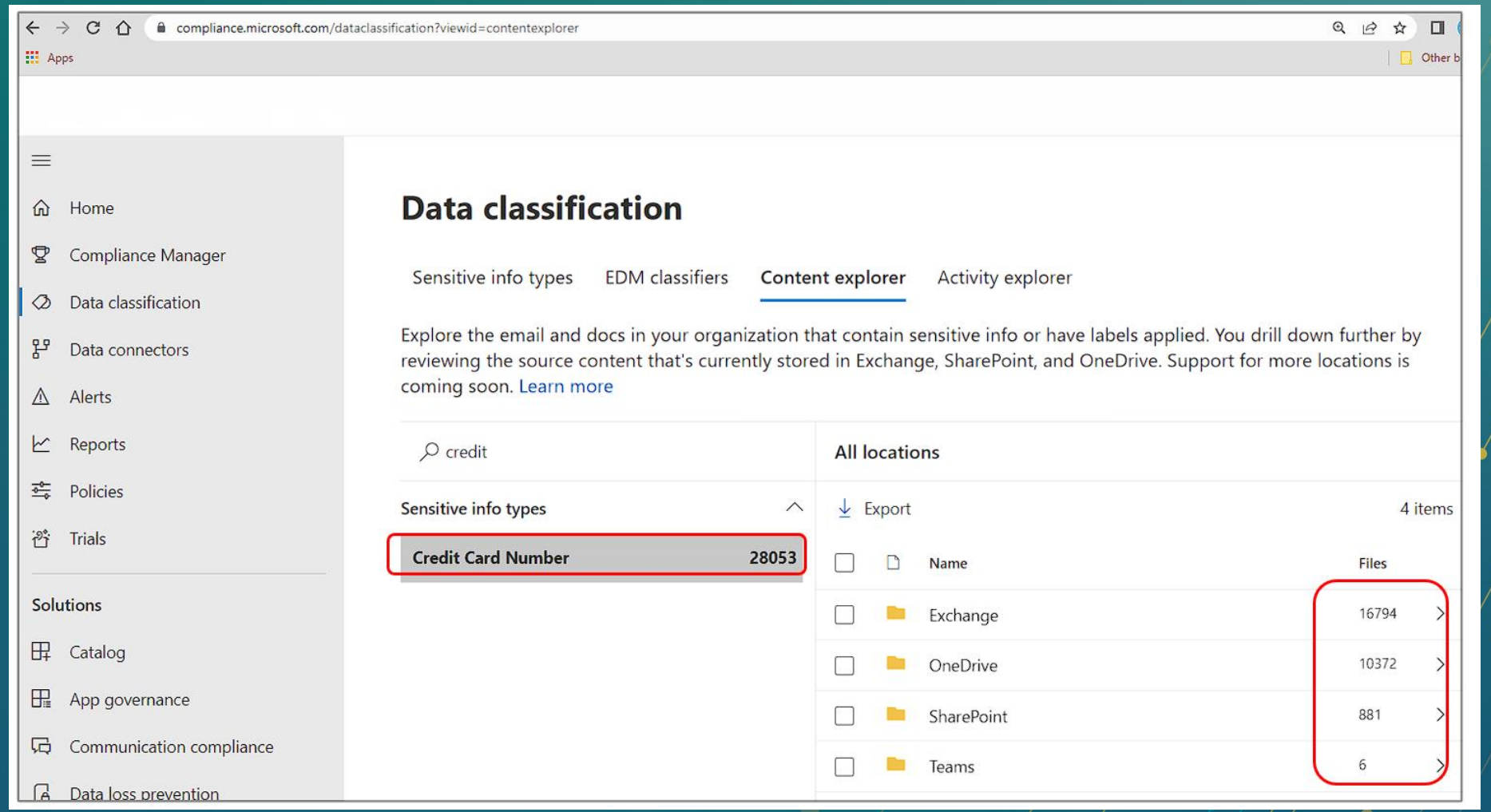
Permissions are set to be like any member (employee) account

NOTE: When an AWS application (e.g., [redacted]) is opened to [redacted] 'ALL', these existing *IAM issues* increase risk exposure!

PCI Security Standards Council

Real-World Examples

Shadow cardholder data environment discovered.



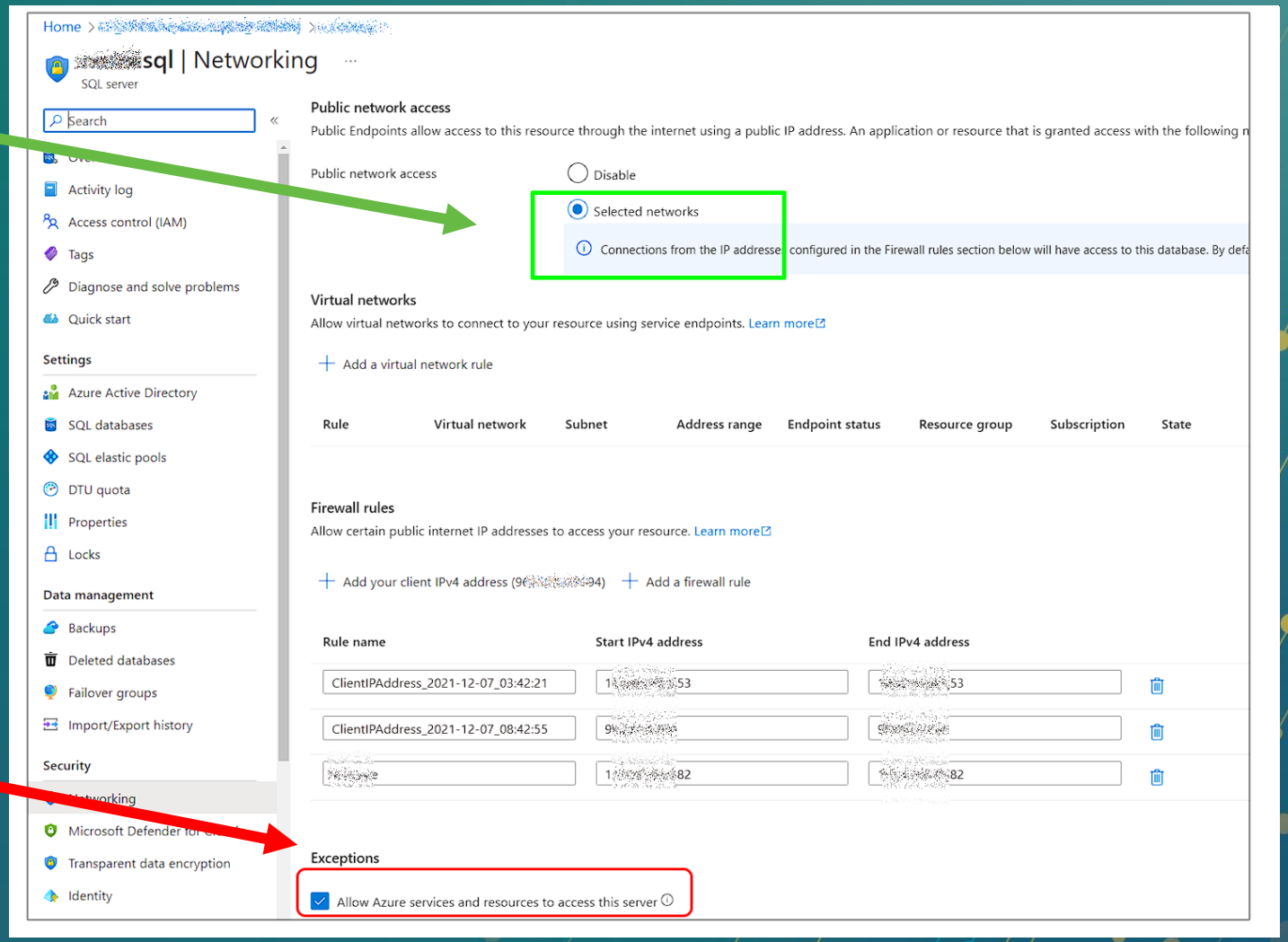
PCI Security Standards Council

Real-World Examples

Database as a Service exposed on the internet (to any other tenant).

A+ for effort!

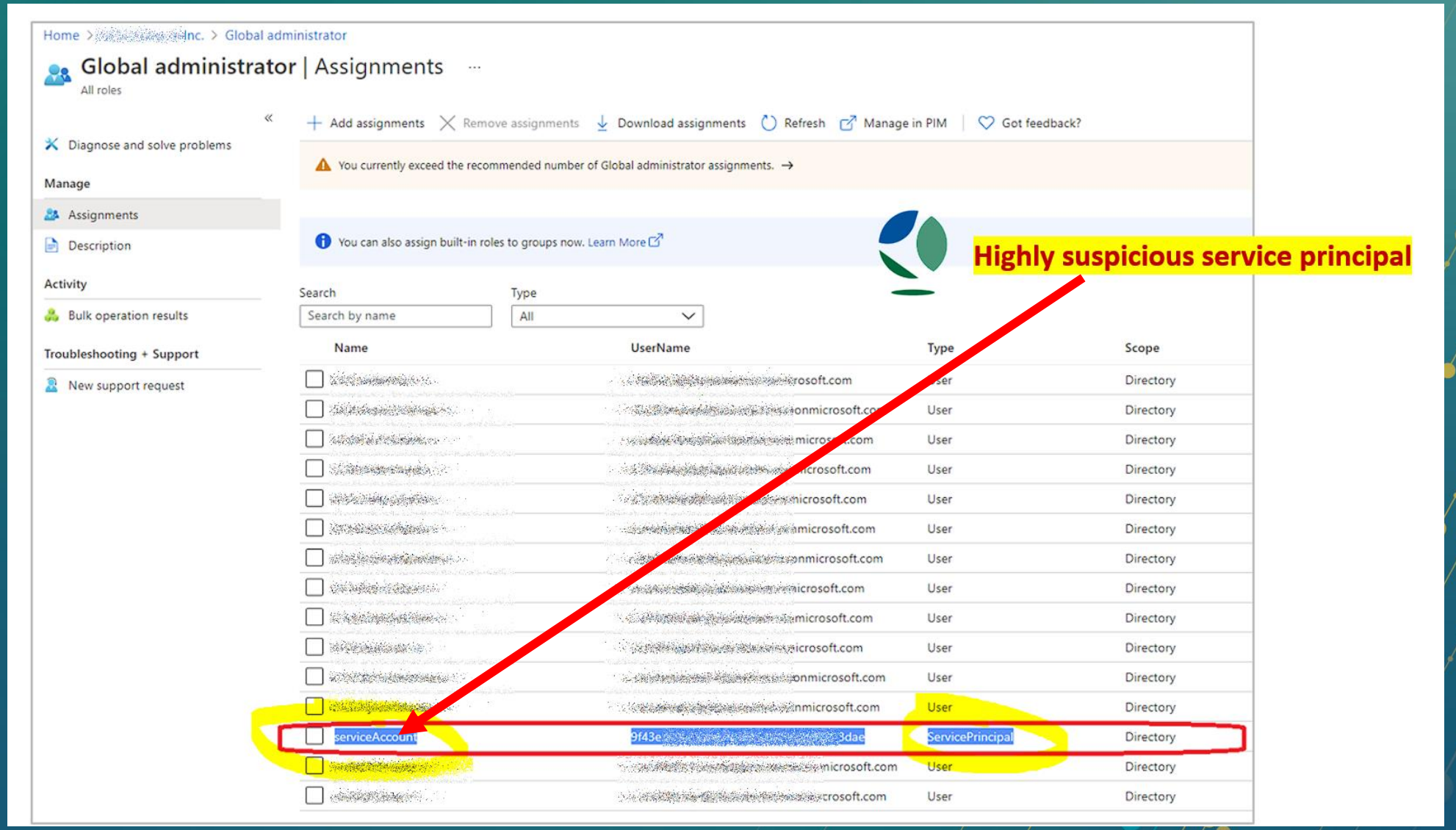
F for execution?



PCI Security Standards Council

Real-World Examples

Suspicious Global Administrator account

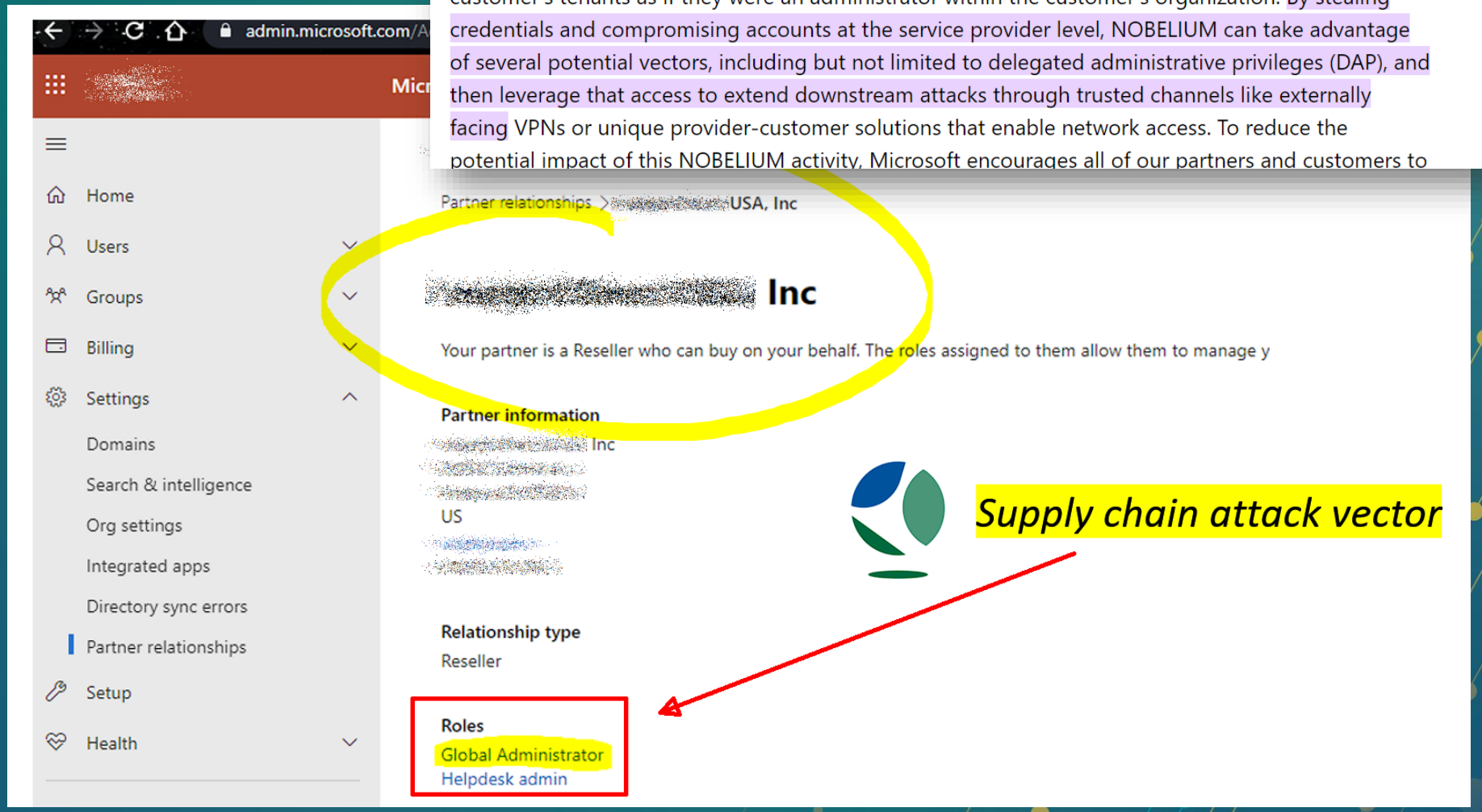


Real-World Examples

Supply chain attack vector via MSP.

NOBELIUM targeting delegated administrative privileges to facilitate broader attacks

In the observed supply chain attacks, downstream customers of service providers and other organizations are also being targeted by NOBELIUM. In these provider/customer relationships, customers delegate administrative rights to the provider that enable the provider to manage the customer's tenants as if they were an administrator within the customer's organization. By stealing credentials and compromising accounts at the service provider level, NOBELIUM can take advantage of several potential vectors, including but not limited to delegated administrative privileges (DAP), and then leverage that access to extend downstream attacks through trusted channels like externally facing VPNs or unique provider-customer solutions that enable network access. To reduce the potential impact of this NOBELIUM activity, Microsoft encourages all of our partners and customers to



Real-World Examples

Leaked AWS API keys on GitHub public repo (owned by developer).

github.com[redacted]src/main/resources/appl

[redacted] / src / main / resources / application.properties

[redacted] Merge branch 'master' of https://github.com/[redacted]

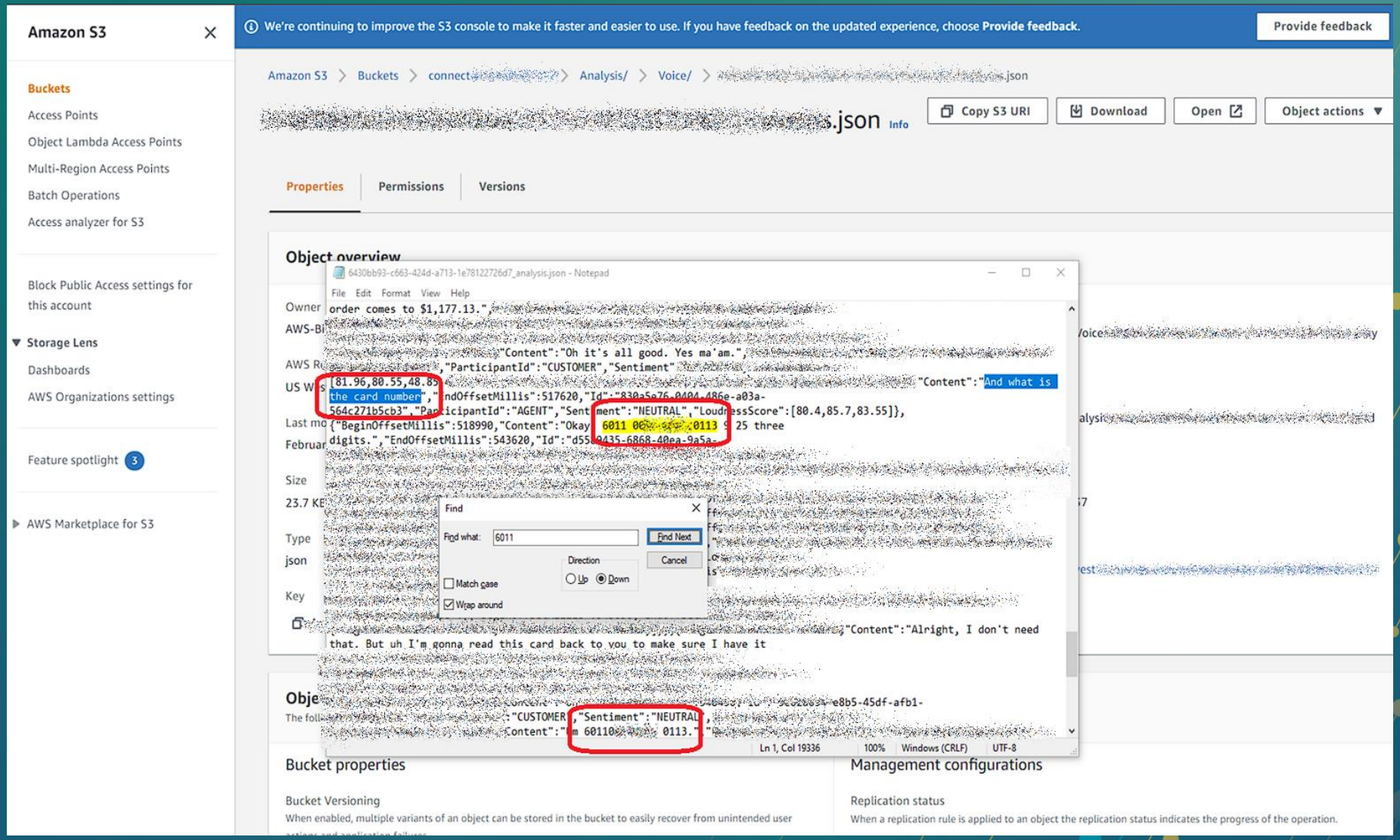
[redacted]

```
21  spring.data.elasticsearch.engine.host=[redacted]
22  spring.data.elasticsearch.engine.port=443
23  spring.data.elasticsearch.engine.username=[redacted]
24  spring.data.elasticsearch.engine.password=[redacted]
```

PCI Security Standards Council

Real-World Examples

Shadow cardholder data environment discovered.



PCI Security Standards Council

Key Takeaways – Clearer Skies Ahead

Let's make cloud less cloudy.

1. Perform a Comprehensive Cloud Security Assessment
2. Perform a Data Discovery, Privacy, Protection Assessment
3. Enable Cloud-Native Security, Compliance, and Governance Tools and/or Use Third-Party Security Solutions (Multicloud)
4. Secure All Authentication Directories and MFA and Vault All Secrets
5. Enable Comprehensive Cloud Control-Plane Logging/Monitoring
6. Create Guardrails or Blueprints to Control Security Misconfigurations
7. Control/Limit Developer Access to the Cloud

PCI Security Standards Council