WIZ

Wiz – OMI..GOD..,,We have your back!

Stories from the Field, for the Field!

Friday, April 15, 2022

1. Who are we and what about Wiz!
2. Stories from our Researchers
3. Demo (Show and Tell)
4. Questions and hopefully some answers

TILBURG

+ sun +

55

2 =

29

https://www.linkedin.com/in/fransvanierland/

2

87

Lisa XL running C.A.S

intra systems
Access. Security. Trust.

AAC Cosmos
ICT Solutions

phoenix technologies
Innovation at the CORE™

SEEBEYOND

Microsoft

VOLMAC

splunk>

WIZ

WIZ

#WhoAmI

Scott .. Aka Scotty! Aka SME for Wiz solutions….

Fun

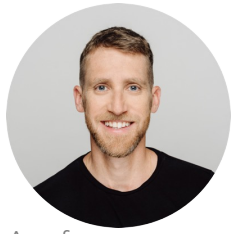
Not European.. Or ?

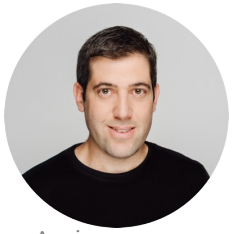
More Fun

Glass is always half full!

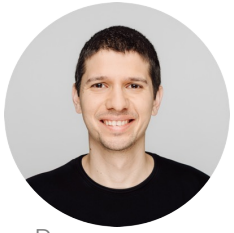
WIZ

Team


Assaf


Ami


Yinon


Roy

Led internal security and cloud products at Microsoft Azure

SEQUOIA

Index Ventures

INSIGHT PARTNERS

By the numbers

500M+
Cloud resources

>1B files
Scanned daily

>$600M
Funding raised

>20%
of the Fortune 500

The fastest growing security startup

UNITED

THE HOME DEPOT

CHIPOTLE MEXICAN GRILL

EA

BARCLAYS

AON

fiserv.

COSTCO WHOLESALE

Chick-fil-A

FOX

Blackstone

salesforce

EY

BlackRock

Morgan Stanley

Honeywell

GitHub

DocuSign

MassMutual

P&G

MARS

Bristol Myers Squibb

Sysco

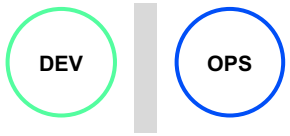
COLGATE-PALMOLIVE

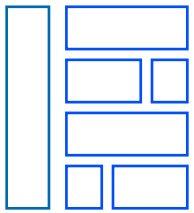
WIZ

Every Company is on a Digital Transformation Journey

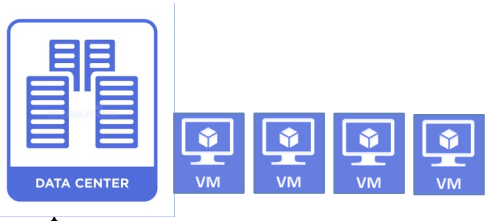
The goal is to improve the availability, reliability, and continuity of applications and services …
What about **risk, vulnerabilities, exposure** and **control**? ….any blind spots or worries?

Retain & Optimize

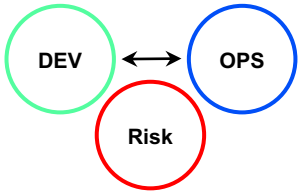


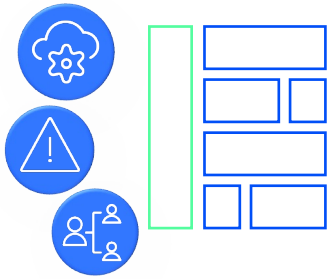


Tightly Coupled Apps,
Slow Deployment Cycles

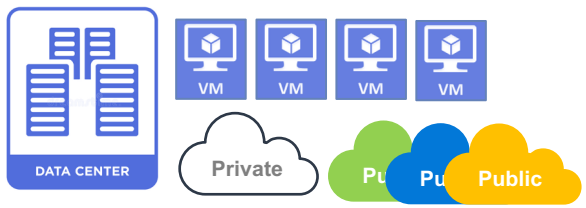


Lift & Shift



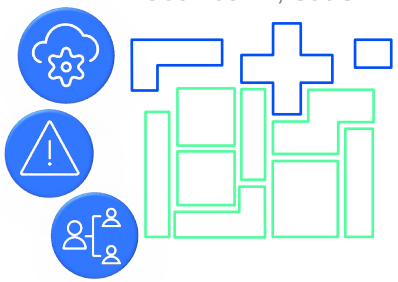


Using
Cloud or Multi cloud IaaS

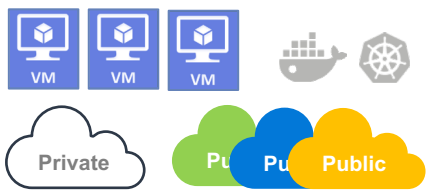


Re-Factor

Cloud Managed e.g. PaaS,
CosmosDB, SaaS

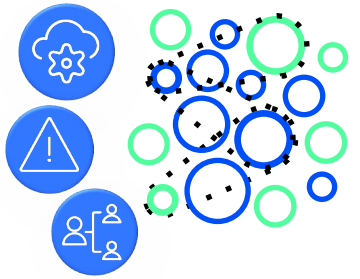


Modular, but
Dependent App Components

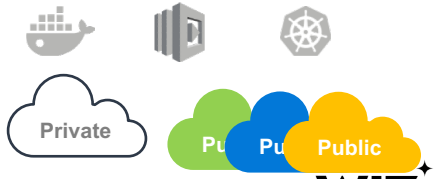


Re-Architect / Cloud-Native

Cloud First Architecture



Loosely Coupled Microservices,
and Serverless Functions



Why is it so hard to find critical risks in the cloud?

Complex environment

Multiple clouds
AWS, Azure, Google, Kubernetes

Multiple architectures
VMs, containers, serverless, PaaS

Thousands of technologies
Growing # of services, applications, libraries

Complex risk

Effective internet exposure
What is effectively exposed to the internet?

Vulnerabilities & misconfigurations
What risks make resources vulnerable?

Lateral movement
What is the effective internal access?

Complex to operationalize

Lack of visibility
No complete picture of the cloud environment

Complex suite of tools
Fragmented across 5+ tools, agents & sidecars

Lengthy time to resolve
Development, DevOps, business units

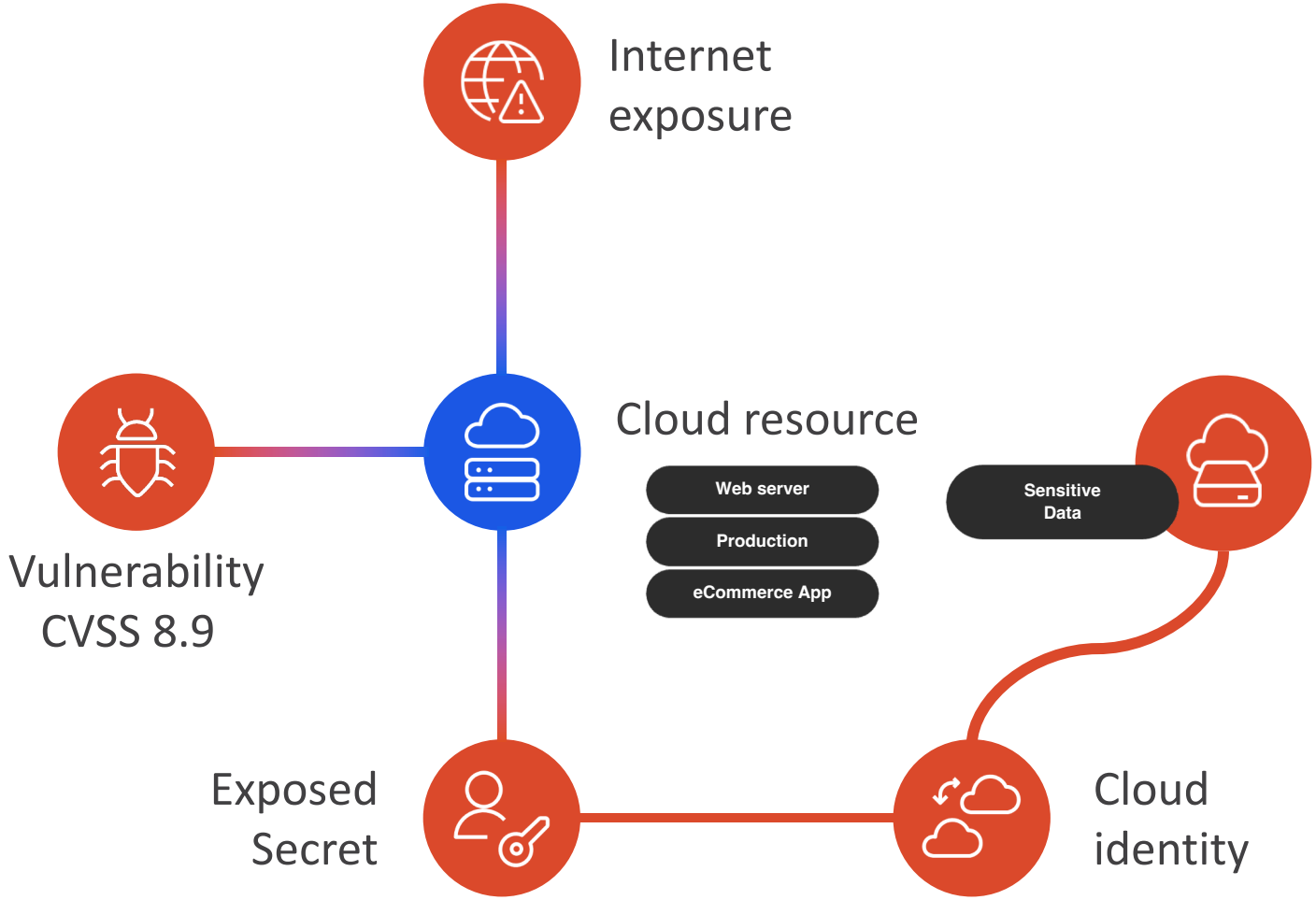
WIZ

How risky is this vulnerability?

Workload context
1. Vulnerabilities
2. Inventory
3. Exposed secrets

Cloud context
1. Resource configuration
2. Networking
3. Identities

Business context
1. Tags
2. Environment
3. Business team



A new approach to cloud security

1 Agentless scan of cloud metadata and workloads

2 Perform a deep cloud assessment

Traditional scanning

Vulnerabilities and missing patches
Misconfigurations
Malware

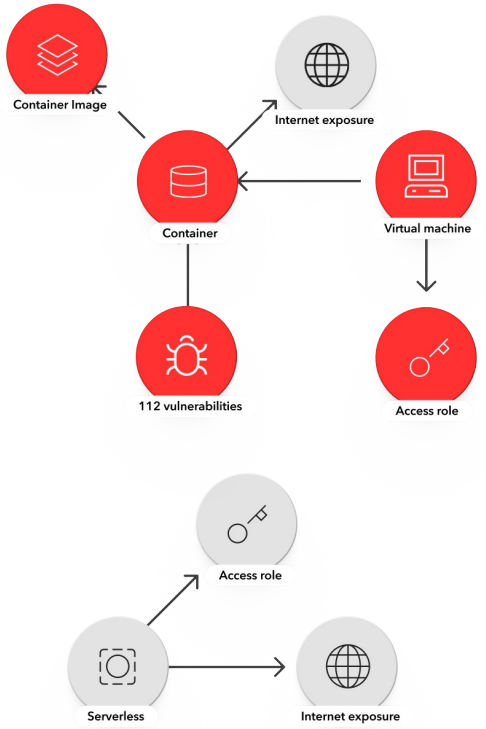
Cloud risk engine

External exposure
Excessive permissions
Exposed secrets
Lateral movement paths

Wiz threat research

Novel cloud vulnerabilities and attacks

3 Identify the most critical risks



4 Proactively harden your cloud

Workflow automation

20+ integrations

Remediation rules

One-click remediation
Automated security response
Remediation guidance

CI/CD and Wiz Guardrails

One policy across the stack
Container and VM image scanning
IaC template scanning

What do we solve

“ An example from the field of research and threat “

WIZ Research

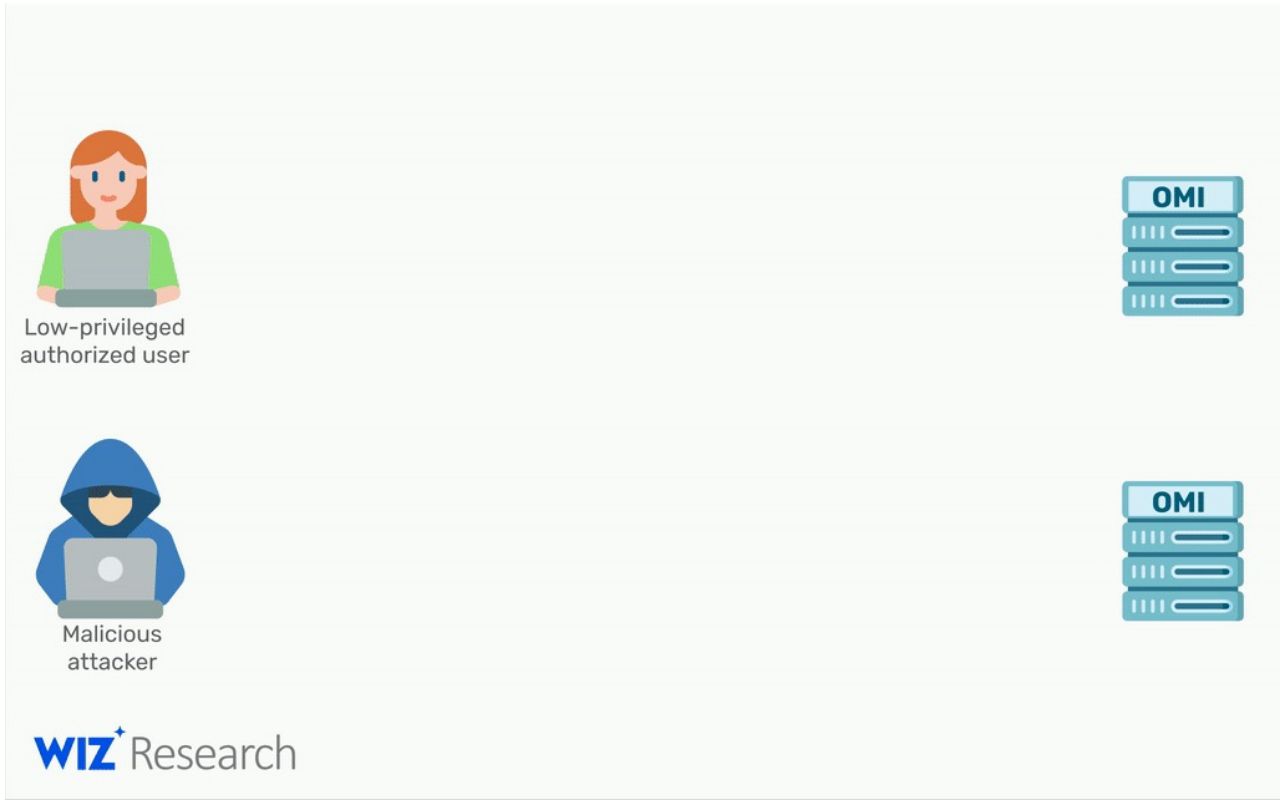
OMI

Why the OMI Attack Surface is interesting to attackers

OMI-GOD

WIZ

Azure Agents , Open Management Infrastructure (OMI) High-severity vulnerabilities



Azure Log Analytics

Azure Monitor

Azure Security Center

65% of sampled Azure customers were exposed

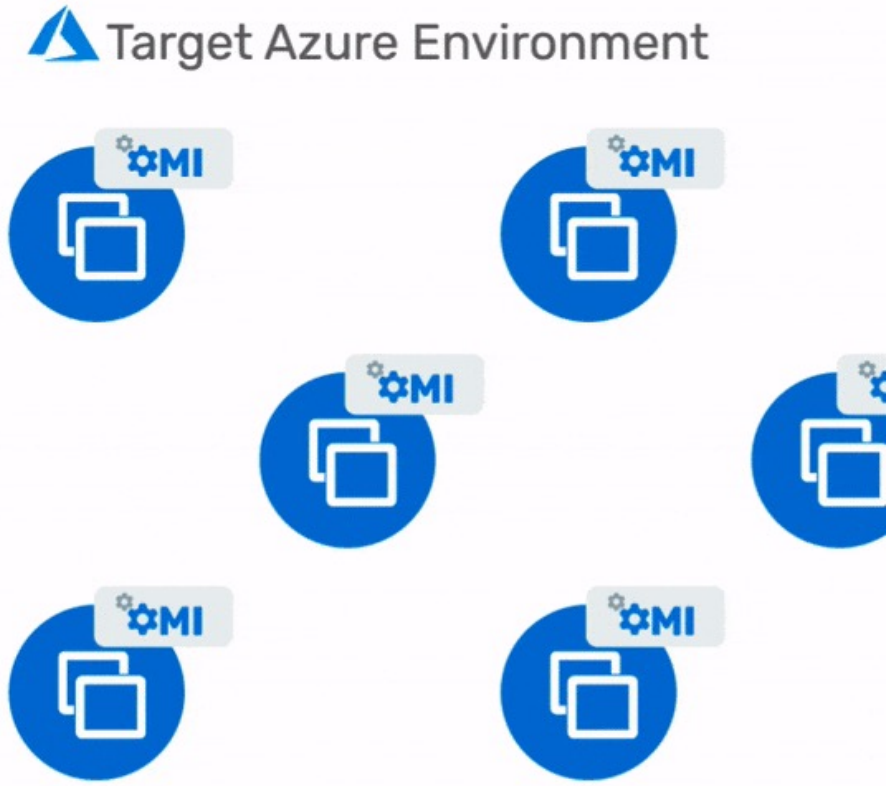
WIZ

Why the OMI Attack Surface is interesting to attackers

The Attackers ToolBox

- CVE-2021-38647 – Unauthenticated RCE as root
- CVE-2021-38648 – Privilege Escalation vulnerability
- CVE-2021-38645 – Privilege Escalation vulnerability
- CVE-2021-38649 – Privilege Escalation vulnerability

WIZ Research



WIZ

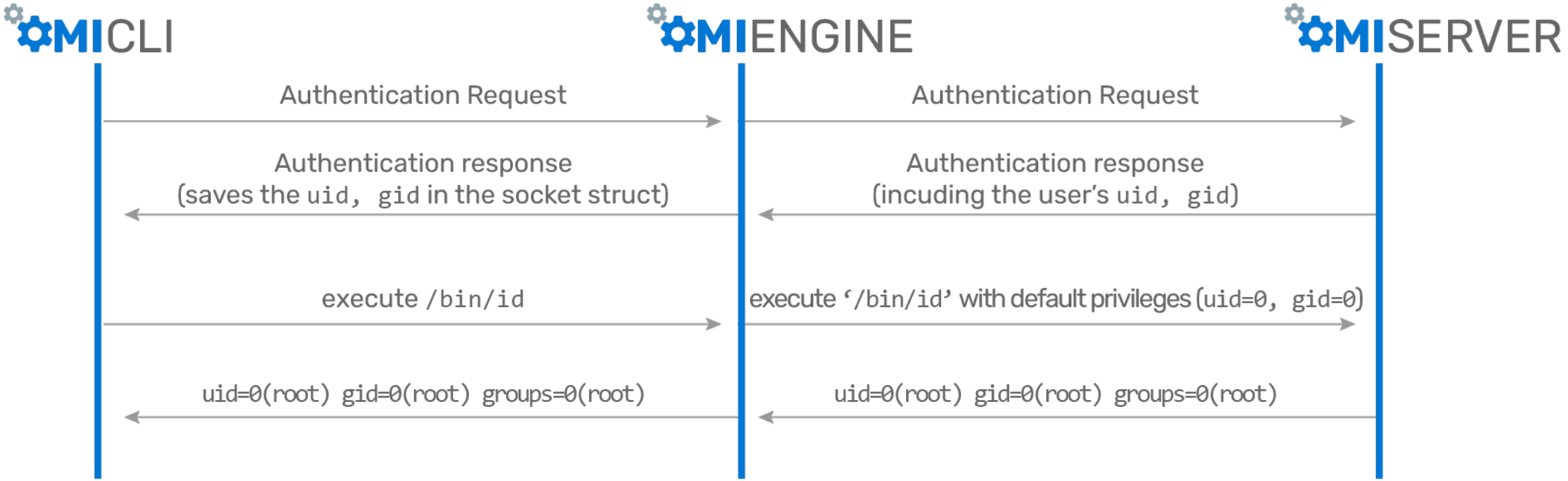
#root. **O-MI-GOD!**

WIZ Research

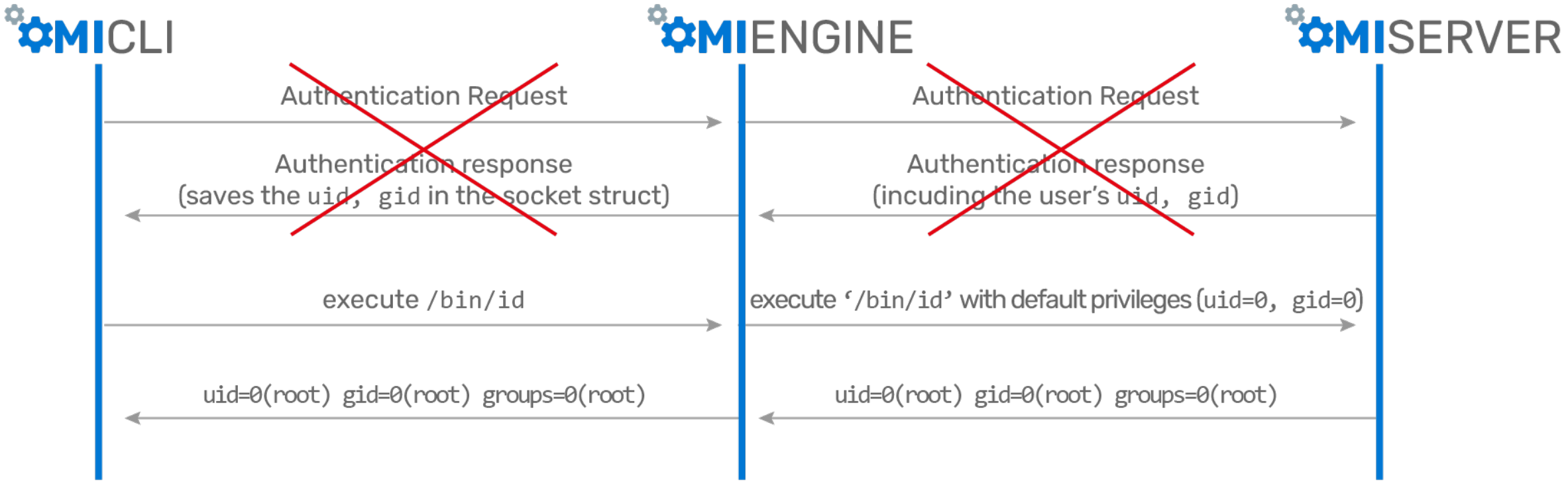
```
@@ -1458,6 +1463,8 @@ static MI_Boolean _ListenerCallback(
1458  1463          h->encryptedTransaction = FALSE;
1459  1464          h->pSendAuthHeader = NULL;
1460  1465          h->sendAuthHeaderLen = 0;
      1466  +       h->authInfo.uid= INVALID_ID;
      1467  +       h->authInfo.gid= INVALID_ID;
```


WIZ

OMI Architecture



OMI Architecture - low privileged user to elevate privileges to root



The rest is history!

CVE-2021-38648 - Local Privilege Escalation **- CVE-2021-38645 - Local Privilege Escalation** **- CVE-2021-38647- Unauthenticated Remote Command Execution**

Disclosure Timeline

June 01, 2021 - Wiz Research Team reported all 4 OMI vulnerabilities to MSRC.
July 12, 2021 - MSRC Confirmed one of the local privilege escalation vulnerabilities (CVE-2021-38648).
July 16, 2021 - MSRC Confirmed one of the local privilege escalation vulnerabilities (CVE-2021-38645).
July 16, 2021 - MSRC Confirmed the remote command execution vulnerability (CVE-2021-38647).
July 23, 2021 - MSRC Confirmed one of the local privilege escalation vulnerabilities (CVE-2021-38649).
August 12, 2021 - Wiz Research Team observed an “Enhanced Security” commit fixing all 4 reported vulnerabilities.
September 8, 2021 – Official patch released.
September 14, 2021 - All 4 vulnerabilities published on September’s Patch Tuesday

```
azureuser@wiz-research-demo:~$ cat /tmp/win
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=1000(azureuser) gid=1000(azureuser) groups=1000(azureuser),4(adm),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),110(lxd)
uid=0(root) gid=0(root) groups=0(root)
```

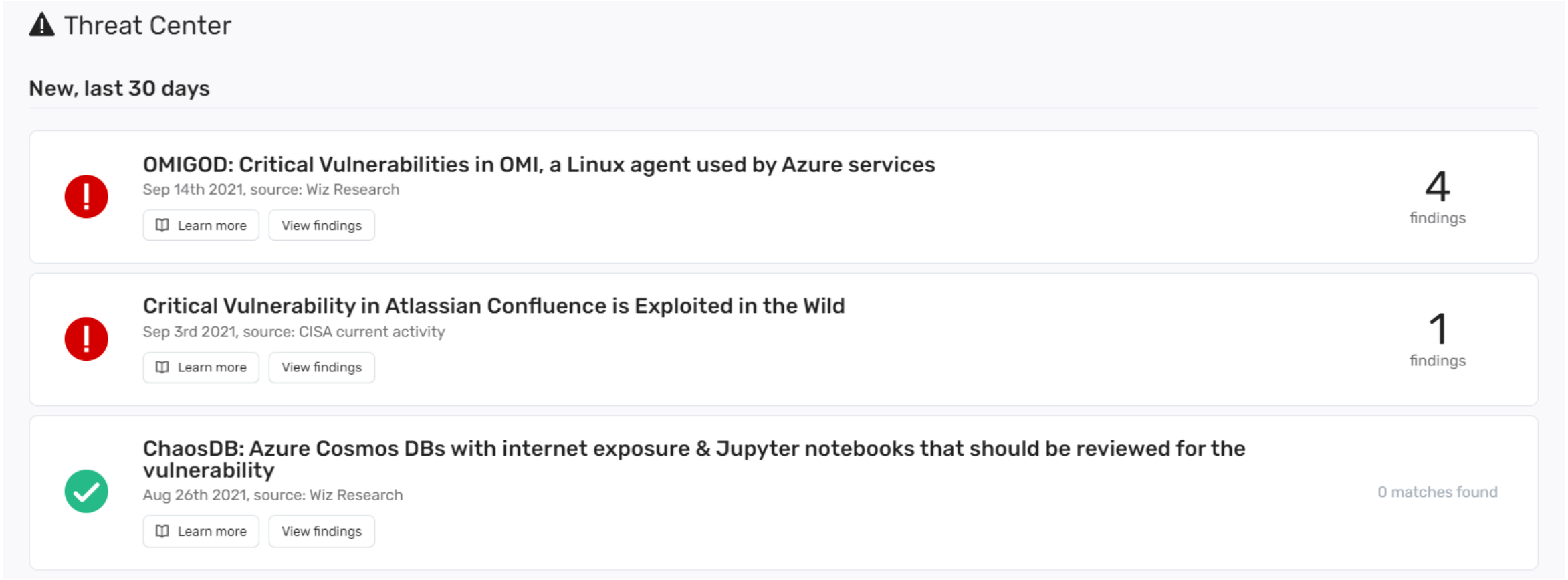
Let me show you……. Beaming you up into the Wiz portal!

Where comes Wiz into play

“ Prevention is better than cure “

What you see is not always reality or ? …. Understanding the details matters……..

Is my environment at risk?



Thank You!

Question ?