Code to Cloud Protection – Microsoft Defender for Cloud: DevOps

Saggie Haim

SAGGIE HAIM

DIRECTOR OF SECURITY SOLUTIONS,
CYBERPROOF

ABOUT ME

I am the Director of Security Solutions at CyberProof, a UST company. Over the past five years, I have focused on resolving complex security challenges and have played a crucial role in building some of the largest cloud-native Security Operations Center (SOC) platforms worldwide. I've actively contributed to Google Security and Microsoft Sentinel product teams by sharing my insights and feedback, driving continuous improvement and innovation in cloud security solutions.

- **15+ Years of Experience In Securing Infrastructure**
- **6 Years of Experience building Cloud Native SOCs**
- **4 Times Azure MVP – Cloud Security & XDR**
- **4 Time Microsoft Certified Trainer**

THE RISE OF THE DEVOPS

The Birth of Agile & Continuous Delivery

(2001 – 2008)

- Agile Manifsto
- CI/CD pipeline

The DevOps Revolution

(2009 – 2015)

- The Term “DevOps” is coined
- Automation became central
- Cloud Computing
- Microservices & Containers

The Difference Between
a Rising Company and a Sinking One:

The Ability to Out-Experiment and Beat Your Competitors in time to market.

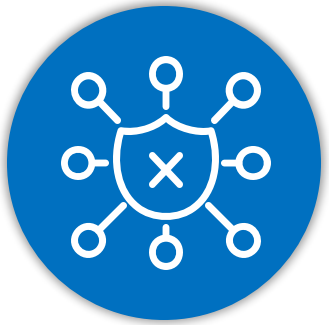
THE CYBER RISKS OF DEVOPS

Leaked Secrets

Misconfiguration

CI/CD

Run-Time Protection



Dependencies

THE SHIFT-LEFT MOVEMENT

Security Becomes a Priority

- Traditional security models were too slow for DevOps.
- Shift-left security emerged → Security checks moved earlier in the development lifecycle.

Cloud-Native Security Tools

- Microsoft Defender for DevOps, Wiz, Prisma Cloud emerged to secure CI/CD pipelines.
- Automation started playing a role in detecting threats early.
- Zero Trust & Policy-as-Code became key principles.

Shift-left security is critical,
but it only solves half the problem.

Security must extend beyond development

Protecting cloud configurations,
workloads, and runtime environments.

Development Security Operation (DevSecOps)

Cloud Security Posture Management (CSPM)

Cloud Workload Protection (CWPP)

Empowers Security teams with the ability to protect applications and resources from code to cloud across multi-pipeline environments

Empowers security teams with continuous visibility and automated remediation of cloud misconfigurations, ensuring compliance, governance, and risk management across multi-cloud environments.

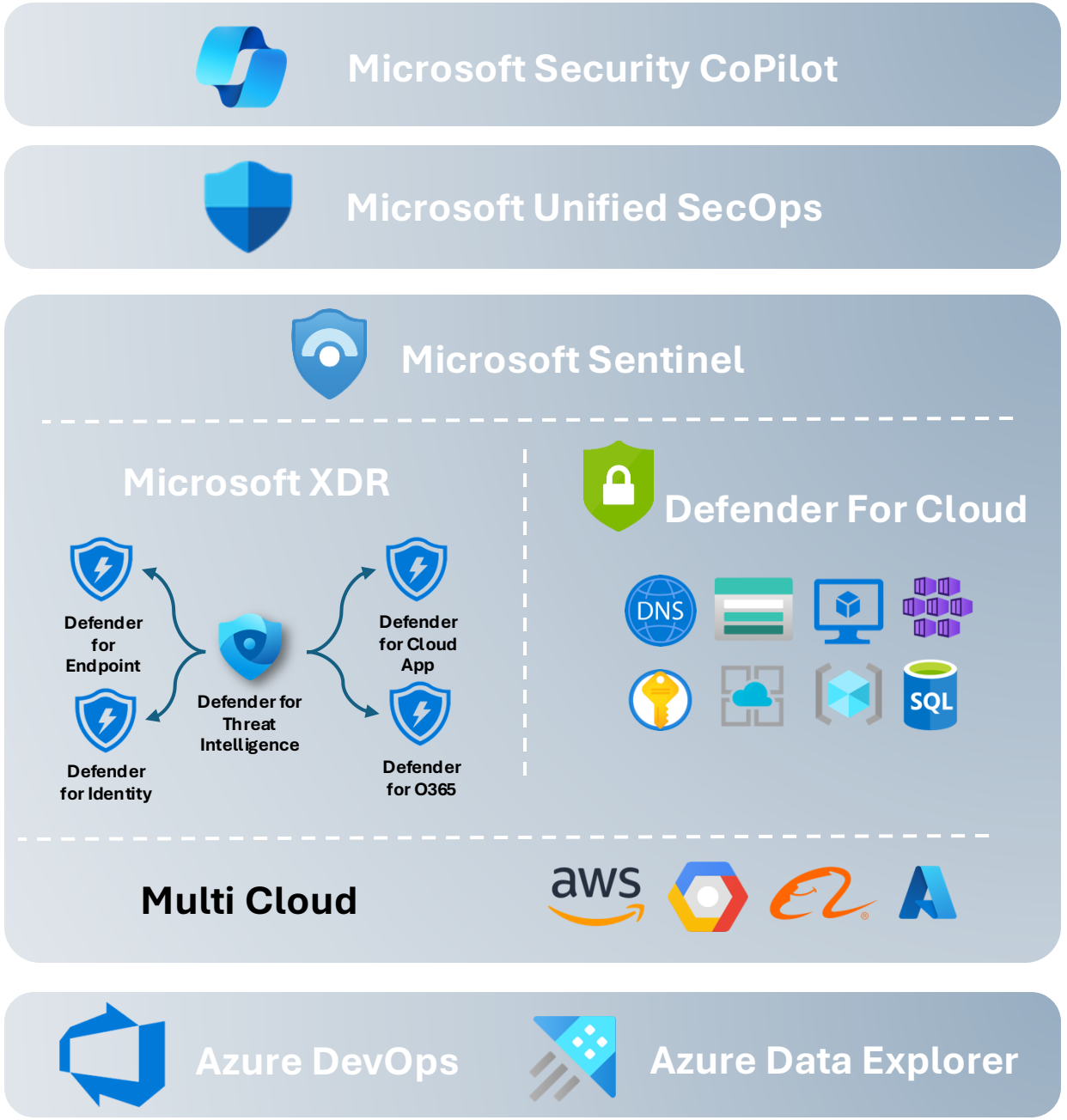
Empowers security teams with real-time threat detection, runtime protection, and automated response for workloads, securing VMs, containers, and serverless environments across hybrid and multi-cloud infrastructures.

The Three Pillars of Defender For Cloud

DevSecOps secures the pipeline, CSPM enforces governance, and CWPP defends workloads in real-time.

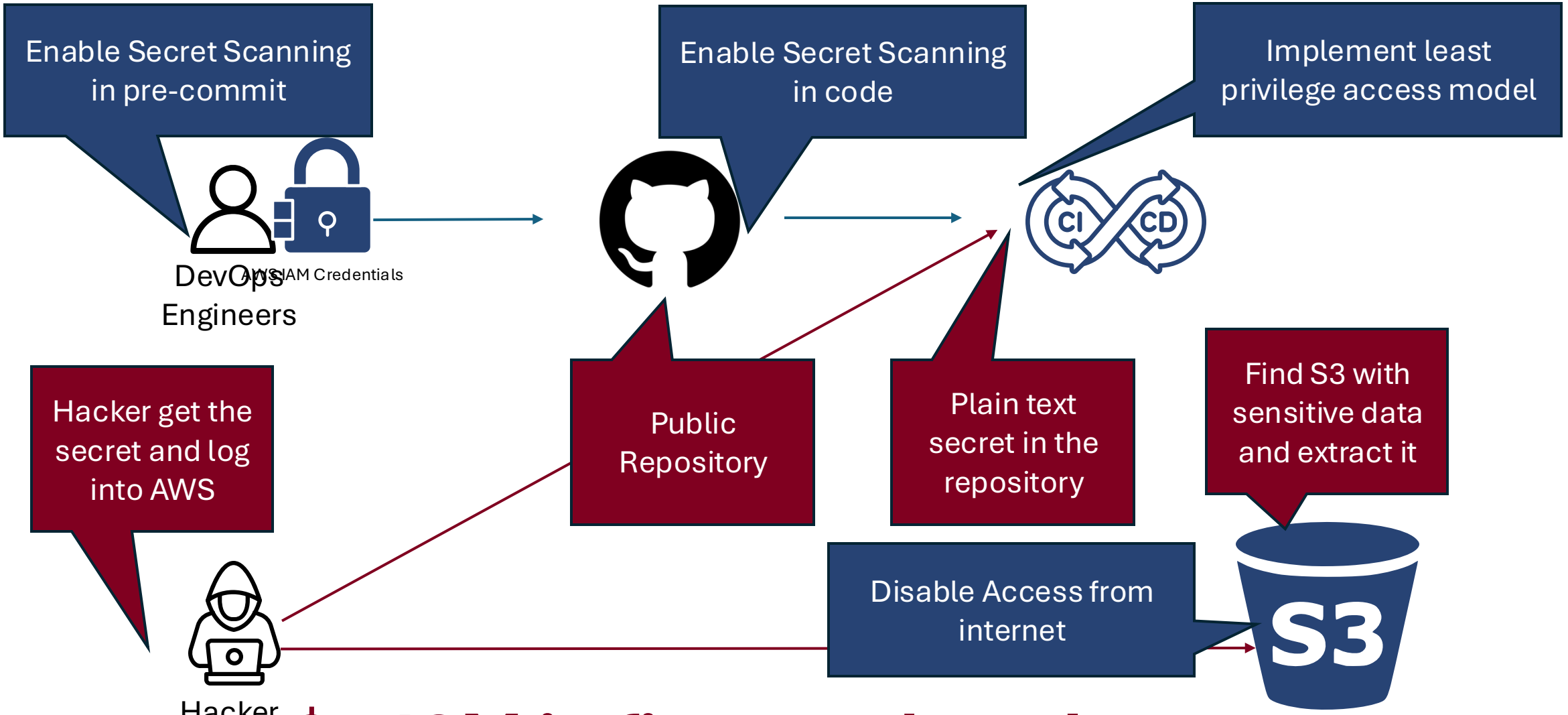
Together, they form Microsoft Defender For Cloud a Cloud Native Application Protection Platform (CNAPP) ensuring that security is continuous, from code to cloud.

So, Where Defender for Cloud sits inside Microsoft Security Platform?



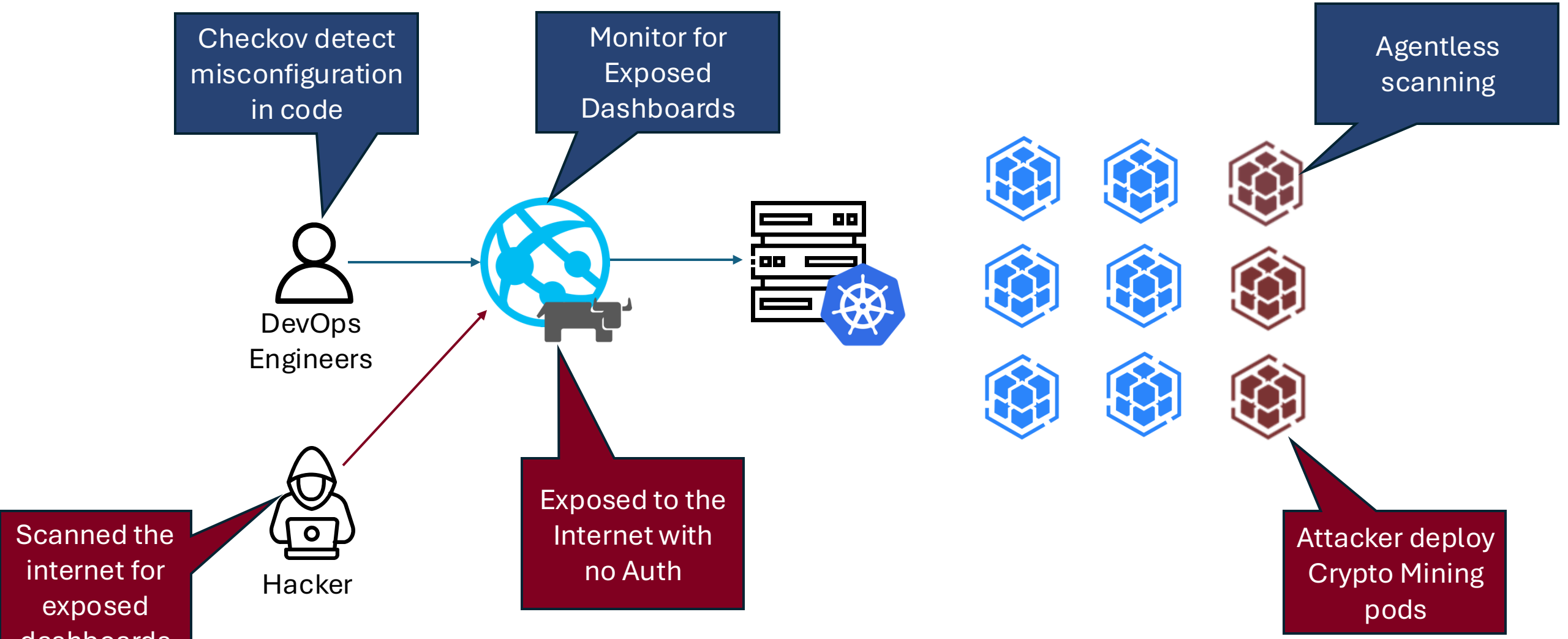
Mitigating Attacks with Defender For Cloud

Uber AWS Credential Leak (2016 & 2022)



$148M in fines and settlements

Tesla Crypto Mining Exploit (2018)



Live Demo

A top tech news company is building a new web portal, with developers using GitHub for development and Azure for cloud hosting.

The website will run inside a container and be hosted on Azure Web Application.

Thanks to top-tier reporting, the company is growing in popularity but with that growth, security risks are increasing.

Let’s explore how Defender for Cloud, with a focus on Defender for Cloud DevOps, can help secure both the developers and the website.