Microsoft Security | Quadra

Entra Permissions Management Workshop

Workshop highlights

Understands how Permissions Creep can impact the attack surface risk in your cloud infrastructure

Gain insights and granular visibility into identities, permissions and resources across your entire multi-cloud infrastructure

Understand how to remediate and prevent identities from being compromised by permissions gap

Over 40K permission exist across the key cloud platforms, and nearly 50% are estimated to be high-risk and could cause catastrophic damage if used improperly (e.g. service disruption, service degradation or data exfiltration) To make matters worse, we've discovered that more than 90% of identities (both human and workload) use less than 5% of the permissions they are granted to perform their daily tasks – leaving the other 95% of unused permissions wide-open to accidental misuse or intentional exploitation of permissions.

Are you aware of over-provisioned identities in your environments?

Excessive Permissions are Expanding your Attack Surface.

The adoption of multicloud is creating new access management challenges for organizations. More and more identities and resources to manage paired with inconsistent access management models across the different clouds cause security teams to struggle with lack of visibility and increasingly complex IT environments. As more services are moved to the cloud, users and workloads continue to accumulate permissions over time. Left unused and unmonitored, these permissions become prime targets for attackers or simple misuse.

Why you should attend

Given the complexity of identities, permissions and resources, it's essential to learn how to ensure the right people are accessing your environment, securely. In this workshop, we'll show you how to address "permissions gap" related risks and how to avoid future permissions creep.

By attending, you can:

Discover

Identify **potential risks** related to identity and see opportunities for improvement.

Improve

Understand how Entra Permissions Management can help you address the **mitigation of the permissions gap**.

Reduce

Reduce the complexity for IAM security teams to manage permissions across multicloud environments.

Plan

Get recommendations and next steps to move forward with **Entra Permissions Management.**

A commissioned study conducted by Forrester Consulting™ on behalf of Microsoft, June 2020

What to expect

Microsoft Entra Permissions Management fully supports all the major cloud service providers, including Google Cloud, AWS, and Microsoft Azure. This tool provides a comprehensive, streamlined view into every action performed by every identity on every resource, so that you can have a look at where your permission risks lie within your multi-cloud infrastructure.

We'll work with you to:

- Shift from static processes that grant permissions based on job roles and assumptions, to a dynamic solution that can right-size permissions based on historical data.
- Recommend effective permissions on demand workflows.
- Recommend automated processes to continuously monitor activity and prevent permissions creep.

We'll customize the workshop based on your organization's needs

Engagement Set up

MEPM Overview

Design and Planning

Customer value conversation

Key results, recommendations and next steps

Demos

Who should attend

The workshop is intended for security decision-makers such as:

- C-SUITE
- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- Identity and or Application owners/decision makers
- IT Security
- IT Operations
- Security Architect
- Security Engineers
- Application business owners

Why Quadra?

Quadra, a Microsoft Global Partner of the Year award winner, helps you improve your security posture by ensuring the principle of least privilege across identities and resources in your multi cloud infrastructure.

.

Contact us today to get started!

Vignesh R | vignesh.r@quadrasystems.net | +91 9655548994 | www.quadrasystems.net