Microsoft Entra Permissions Management

Proof of Concept (PoC) overview

PoC | Stakeholders

Common customer stakeholders

We will engage the following stakeholders at specific stages of the POC:

- Identity team: Microsoft Entra ID Global Administrator
- Cloud Infrastructure team: Architects and Operations team for Azure, AWS, and GCP environments
- InfoSec team: Architects and Operations
- Incident Response team
- Security Assurance / Audit team
- Target resource technical owners (e.g. administrators/developers)

Microsoft stakeholder

- PoC driver: Microsoft engineer who will guide you during the PoC process

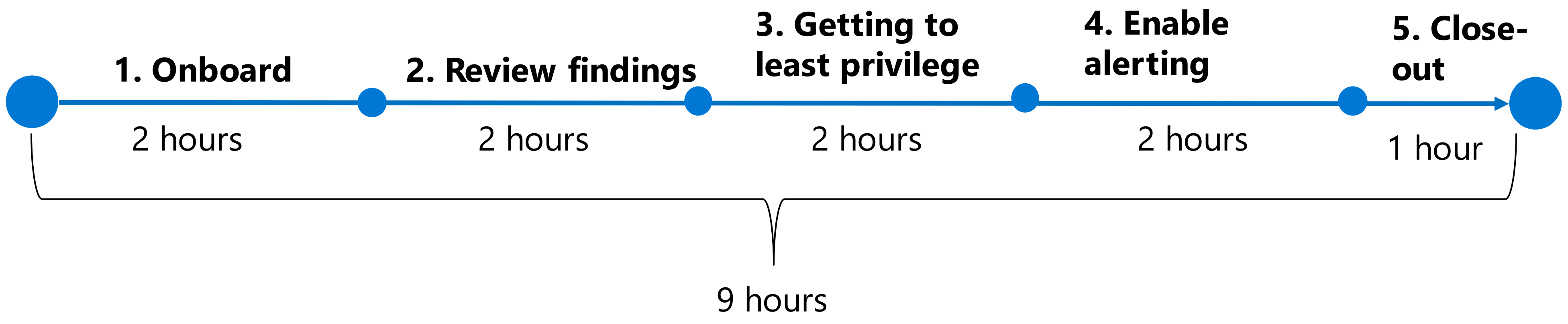
Proof of concept (PoC) | Goals

Demonstrate the value of Microsoft Entra Permissions Management in your environment:

- **Discover** overprivileged accounts and resources in your Azure, AWS, and GCP environments
- **Remediate:** Identify most critical and low hanging items for your teams and right-size permissions and implement least privilege over the next 30 days
- **Monitor / Alert:** Enable alerts and monitoring for your SOC team

PoC | Timeline

Delivery stages



Logistics

- Each stage will only require participation of a subset of stakeholders from customer
- There needs to be a 24-hour period after onboarding to complete data collection
- We recommend phase 2-4 to be done as close together as feasible

How does it work?

Delivery stages

- Phase 1: Onboard – 2 hours
- Phase 2: Review Findings – 2 hours
- Phase 3: Getting to Least Privilege – 2 hours
- Phase 4: Enable Alerting – 2 hours
- Close out : 1 hour

Logistics

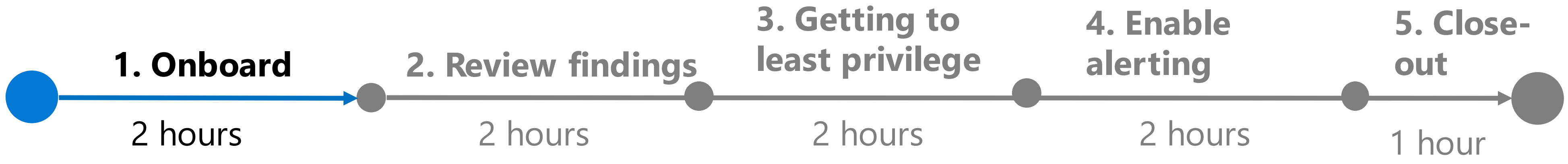
- There needs to be a 24-hour period after onboarding to complete initial data collection and analysis
- We recommend phase 2-4 to be done as close together as feasible

PoC | Pre-work

Identify resources to onboard. Recommendations

- Enable production resources to discover meaningful issues (this will not change permissions)
- Also enable non-production or productions resources to exercise remediations/right-sizing (this might change permissions)
- Onboard Azure, AWS, and GCP resources to better see cross-cloud management benefits
- Identify technical owners of the PoC resources, in case remediation/investigations are needed

PoC | Phase 1: Onboard



1. Onboard
2 hours

2. Review findings
2 hours

3. Getting to least privilege
2 hours

4. Enable alerting
2 hours

5. Close-out
1 hour

Education session (1 hour): **Introduction to EPM**

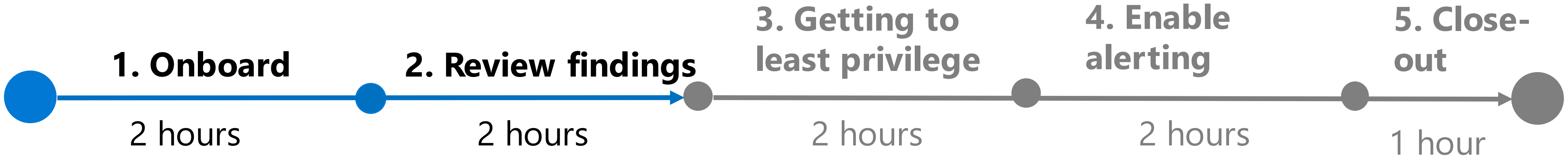
- Who? → All teams

Working session

1 to 2 hours, depending on what clouds and resources in scope

Role	Responsibility
Microsoft Entra ID Global Admin	Activate Trial and initial setup
Azure Ops team	onboard Azure resources
AWS Ops team	onboard AWS resources
GCP Ops team	onboard GCP resources
All above mentioned roles	validate data collection started

PoC | Phase 2: Review findings



1. Onboard 2 hours

2. Review findings 2 hours

3. Getting to least privilege 2 hours

4. Enable alerting 2 hours

5. Close-out 1 hour

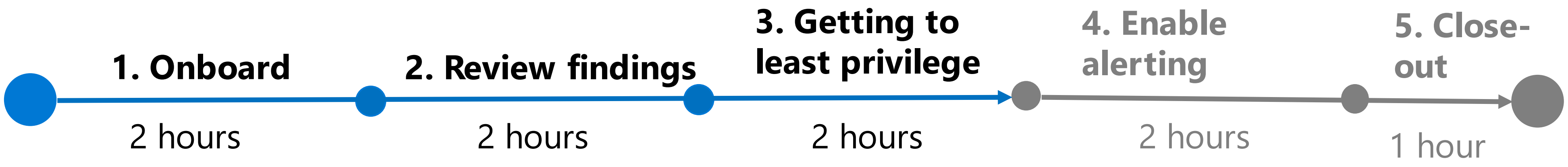
Working session (2 hour): 24 hours after onboarding

Role	Responsibility
Cloud infrastructure architects	→ Review Dashboard and discuss Permission Creep Index → Review Permissions Analytics Report → Triage and prioritize findings to go after for next 30 days

Report out session (1 hour)

Role	Responsibility
InfoSec Architects, Cloud Infrastructure Architects, Incident Response, Audit, Resource Owners	→ Review Dashboard and discuss Permission Creep Index and 30-day finding prioritized plan

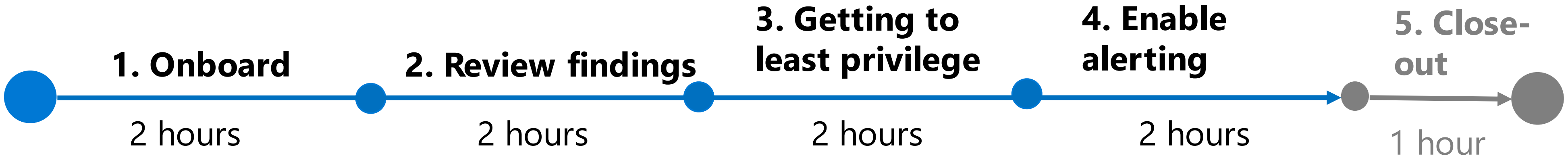
PoC | Phase 3: Getting to least privilege



Working session (2 hour)

Role	Responsibility
Cloud infrastructure architects/ops	→ Understand how to use reports to identify least privilege → Enable Permissions on demand for target resources Note: This will change permissions.

PoC | Phase 4: Enable alerting



1. Onboard — 2 hours

2. Review findings — 2 hours

3. Getting to least privilege — 2 hours

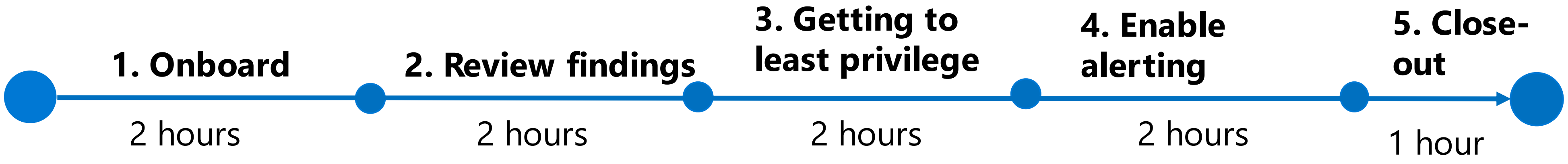
4. Enable alerting — 2 hours

5. Close-out — 1 hour

Working session (2 hour)

Role	**Responsibility**
InfoSec Ops team	→ Enable rule-based alerts → Enable statistical anomaly alerts → Enable permission analytic alerts → Enable activity-based alerts (Optional)
InfoSec Ops team / Audit team	Generate reports on a regular schedule

PoC | Phase 5: Close-out



Wrap-up session (1 hour)

Who?

→ All teams

→ Leadership team

Goal

- Present top findings to leadership
- Discuss strategy to further implement
- Fill out PoC closeout survey

Phase 1: Onboard

Education session – 1 hours

1. All teams: Introduction to EPM

Working session – (1 to 2 hours, depending on what clouds and resources in scope)

1. Azure AD Global Admin: Activate Trial and initial setup
2. Azure Ops team: Onboard Azure resources
3. AWS Ops team: Onboard AWS resources
4. GCP Ops team: Onboard GCP resources
5. Validate data collection started

Phase 2: Review Findings

After 24 hours of onboarding: Working session – 2 hours

1. Cloud Infra Architects: Review Dashboard and discuss Permission Creep Index
2. Cloud Infra Architects: Review Permissions Analytics Report
3. Cloud Infra Architects: Triage and Prioritize findings to go after for next 30 days.

Report Out session – 1 hour

4. InfoSec, Incident Response, Audit, Resource Owners: Present critical findings per triage

Phase 3: Getting to Least Privilege

Working session – 2 hours

1. Cloud infra architects/ops: Understand how to use reports to identify least privilege
2. Cloud infra architects/ops: Enable Permissions on demand for target resources (note: This will change permissions)

Phase 4: Enable Alerting

Closeout session – 2 hours

1. SOC team: Enable rule-based alerts
2. SOC team: Enable statistical anomaly alerts
3. SOC team: Enable permission analytic alerts
4. SOC team / Audit: Generate reports on a regular schedule
5. SOC team: Enable activity-based alerts (Optional)

PoC Closure

Wrap-Up session: 1 hour

1. Present top findings to leadership
2. Build strategy to implement
3. Fill out survey

Thank you!

Microsoft Security