SPYGLASS MTG

A Women Owned/Women Led Company

Azure Security Assessment

A 3-Week/$35k Offer

Microsoft
Solutions Partner

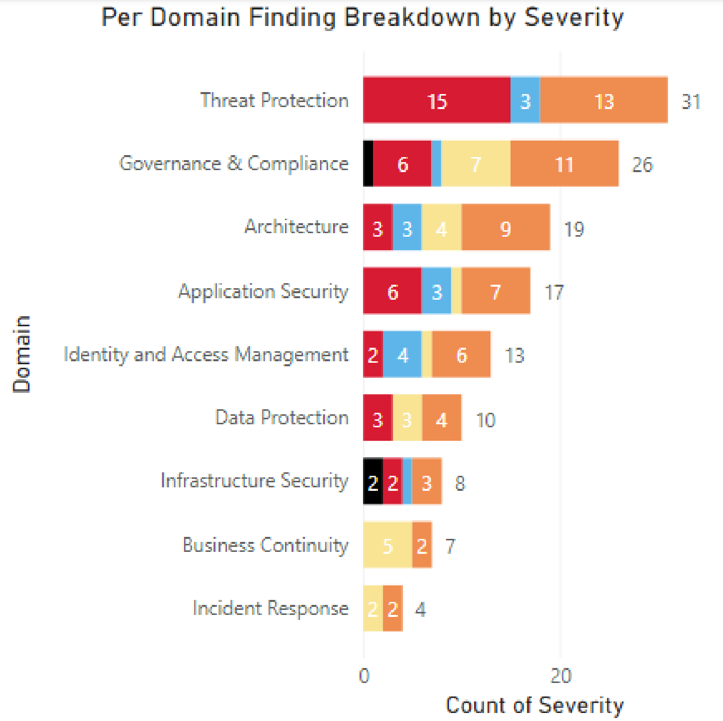
Infrastructure Azure
Data & AI Azure
Digital & App Innovation Azure
Modern Work
Security

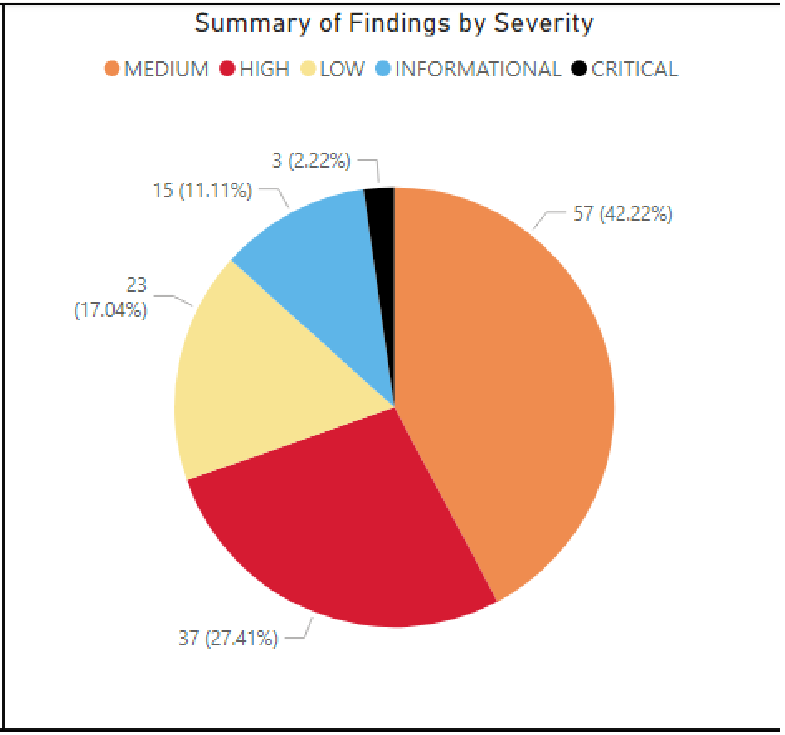
Azure Security Assessment

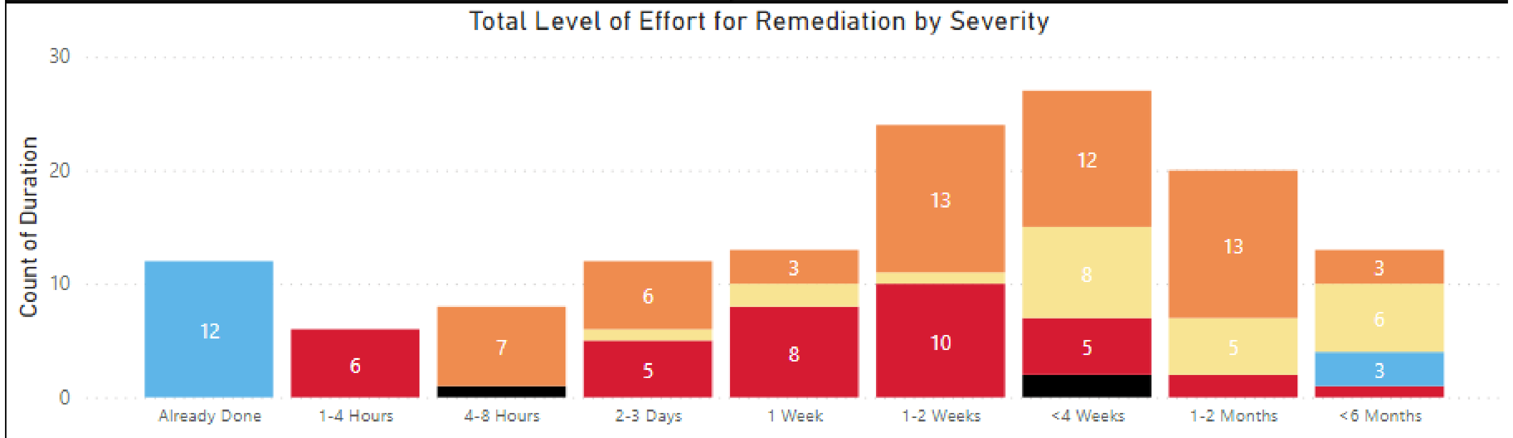
- Objectives
  - Identity current environment gaps in the Azure environment and workloads
  - Evaluate security domains against the Azure environment and workloads
  - Generate prioritized list of issues that need to be addressed
  - Outline recommendations to continue to improve security in the environment

- Summary of High Level Findings
  - Governance of Azure environment needs to be improved to better control what is deployed and how it is used.
  - Network security controls needs to be refactored to move to a zero trust module for network traffic.

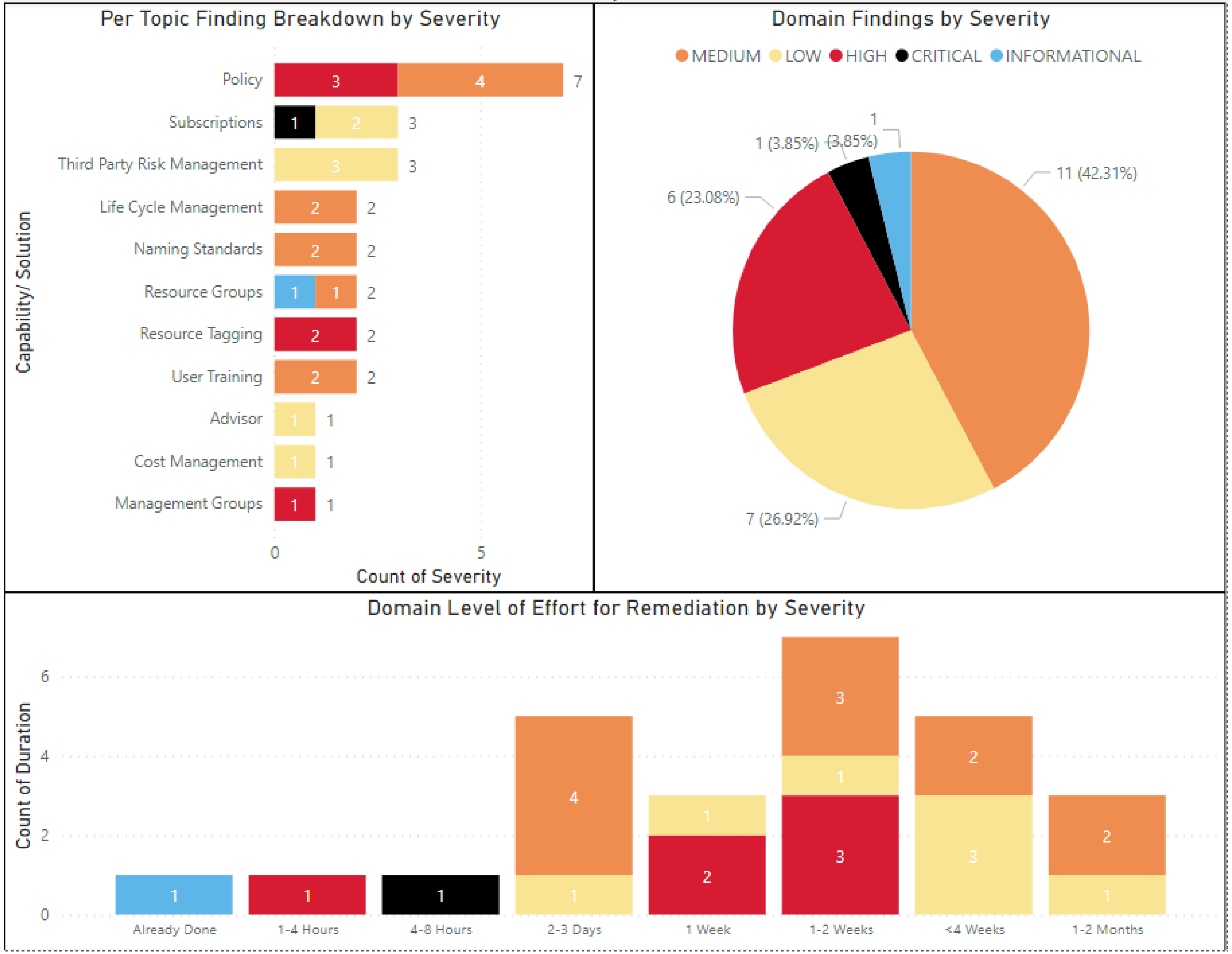
Security Domain Summary


Per Domain Finding Breakdown by Severity


Summary of Findings by Severity


Total Level of Effort for Remediation by Severity

Governance and Compliance

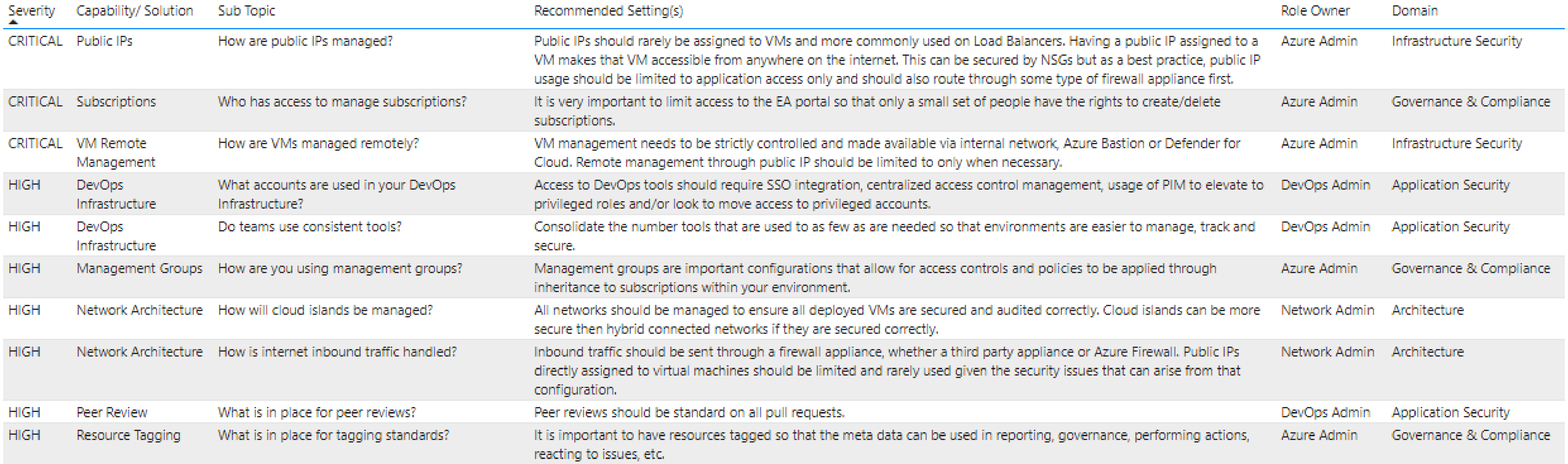


Per Topic Finding Breakdown by Severity

Domain Findings by Severity

Domain Level of Effort for Remediation by Severity

Roadmap of Prioritized Findings - Immediate



Severity	Capability/ Solution	Sub Topic	Recommended Setting(s)	Role Owner	Domain
CRITICAL	Public IPs	How are public IPs managed?	Public IPs should rarely be assigned to VMs and more commonly used on Load Balancers. Having a public IP assigned to a VM makes that VM accessible from anywhere on the internet. This can be secured by NSGs but as a best practice, public IP usage should be limited to application access only and should also route through some type of firewall appliance first.	Azure Admin	Infrastructure Security
CRITICAL	Subscriptions	Who has access to manage subscriptions?	It is very important to limit access to the EA portal so that only a small set of people have the rights to create/delete subscriptions.	Azure Admin	Governance & Compliance
CRITICAL	VM Remote Management	How are VMs managed remotely?	VM management needs to be strictly controlled and made available via internal network, Azure Bastion or Defender for Cloud. Remote management through public IP should be limited to only when necessary.	Azure Admin	Infrastructure Security
HIGH	DevOps Infrastructure	What accounts are used in your DevOps Infrastructure?	Access to DevOps tools should require SSO integration, centralized access control management, usage of PIM to elevate to privileged roles and/or look to move access to privileged accounts.	DevOps Admin	Application Security
HIGH	DevOps Infrastructure	Do teams use consistent tools?	Consolidate the number tools that are used to as few as are needed so that environments are easier to manage, track and secure.	DevOps Admin	Application Security
HIGH	Management Groups	How are you using management groups?	Management groups are important configurations that allow for access controls and policies to be applied through inheritance to subscriptions within your environment.	Azure Admin	Governance & Compliance
HIGH	Network Architecture	How will cloud islands be managed?	All networks should be managed to ensure all deployed VMs are secured and audited correctly. Cloud islands can be more secure then hybrid connected networks if they are secured correctly.	Network Admin	Architecture
HIGH	Network Architecture	How is internet inbound traffic handled?	Inbound traffic should be sent through a firewall appliance, whether a third party appliance or Azure Firewall. Public IPs directly assigned to virtual machines should be limited and rarely used given the security issues that can arise from that configuration.	Network Admin	Architecture
HIGH	Peer Review	What is in place for peer reviews?	Peer reviews should be standard on all pull requests.	DevOps Admin	Application Security
HIGH	Resource Tagging	What is in place for tagging standards?	It is important to have resources tagged so that the meta data can be used in reporting, governance, performing actions, reacting to issues, etc.	Azure Admin	Governance & Compliance