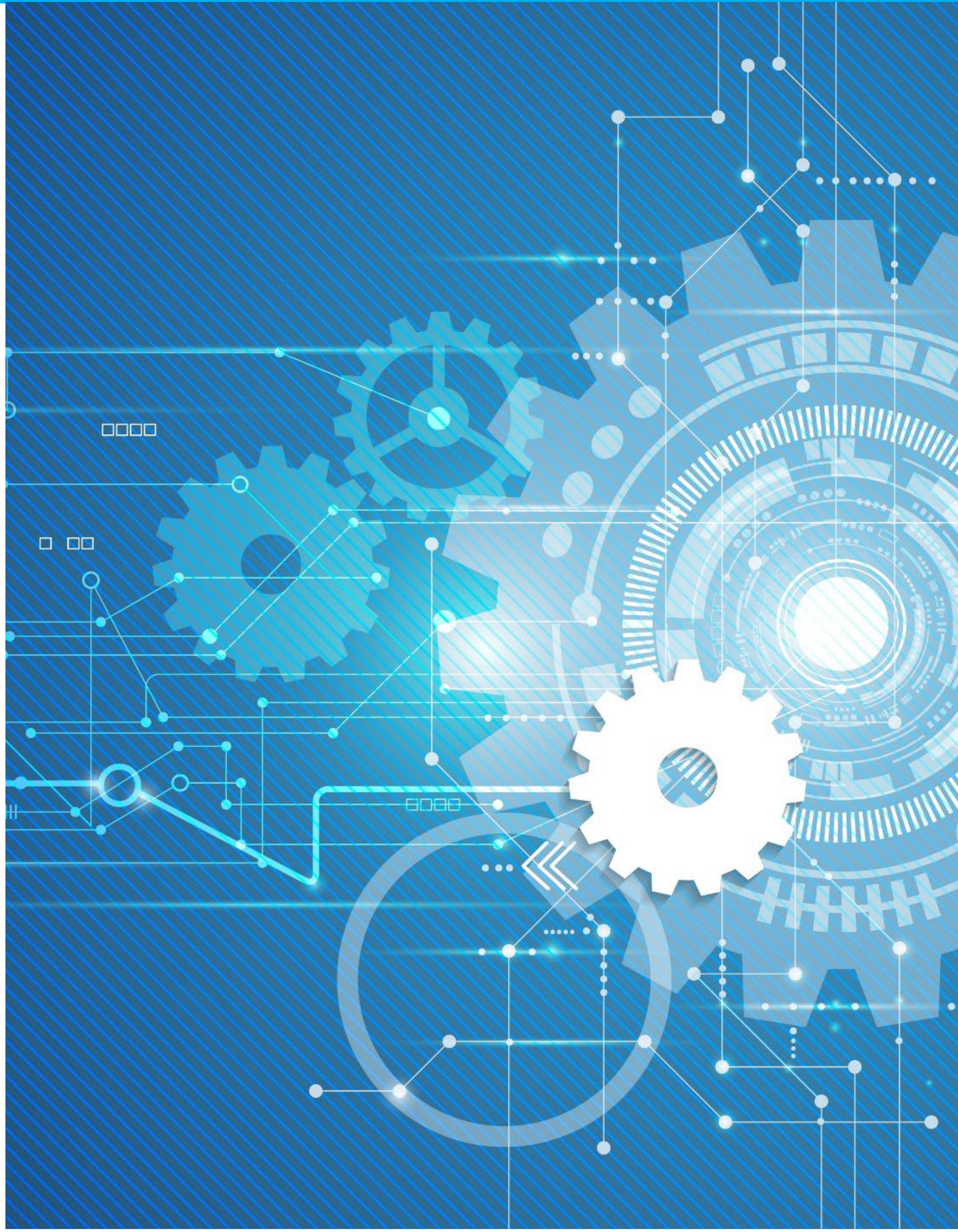
SPYGLASS MTG

Women Owned/Women Led

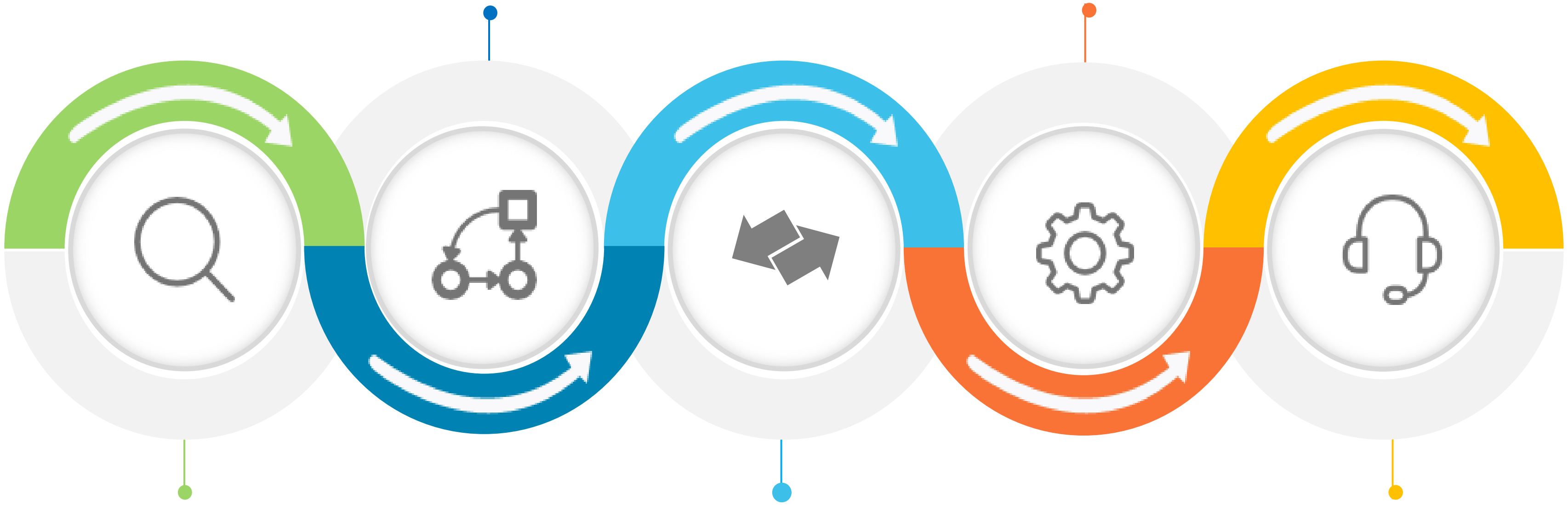
Microsoft Sentinel in 30 Days: 4-Week Implementation

Microsoft Sentinel in 30 Days

- Objectives
  - Design and deploy Microsoft Sentinel in scalable and secure architecture that allows for easily onboarding new log sources and managing Sentinel content for SOC operations.
- Approach
  - Understand current SIEM environment and strategy for SOC.
  - Ensure the scalable and secure Microsoft Sentinel architecture.
  - Onboard initial log sources and develop common patterns for onboarding additional log sources.
  - Ensure analytic rules/workbooks/queries are in place and part of SOC processes to ensure value is seen from initial Sentinel usage.
- Timeframe
  - 4-Week / $35k implementation



Spyglass Deployment Process



1 – ANALYSIS & INVENTORY

- Review current SIEM platform
- Understand security operations strategy
- Discuss current cloud strategy

2 – DESIGN & DEPLOYMENT

- Design Microsoft Sentinel Architecture
- Deploy environment with IaC

3 - ONBOARDING

- Configure log ingestion
- Migrate SIEM content to Sentinel
- Customize Sentinel content

4 - INTEGRATION

- Integrate with SOC processes
- Define new tasks and processes

5 - RESPONSE

- SOC Knowledge Transfer
- Alert investigation and remediation
- Review response actions that can be automated

Thank You

info@spyglassmtg.com