SecWise PROTECT

M365 Threat
Protection Solutions

Koen.Jacobs@secwise.be

Gold
Microsoft Partner
Security

Microsoft

SecWise

SECWISE PROTECT

HOW TO DETECT AND PROTECT AGAINST SOPHISTICATED MALWARE & HACKING ATTACKS?

SecWise

SecWise Protect offering:

Solution Description

- Implement **advanced mail security** to protect against phishing and drive by download (malicious URLs)attacks using Office ATP security
- Improve visibility into the usage of **Shadow IT** and **cloud applications** (CASB)
- Provide visibility in on prem **AD security** (privileged access management, lateral movement paths , …)
- Centralized view on all security controls to **manage** the Microsoft Defender ATP products **on a day to day basis**.

Service Options

- Light
- Elevated
- Advanced

Solution Goal

- Improve **malware protection**
- **Protect** against **phishing** and drive by download attacks
- Improve visibility into the usage of **Shadow IT** and **cloud applications**
- Provide visibility in on prem **domain security**
- **Centralized view** on all security controls

SecWise Protect flavours

Light

- Enable basic mail security policies:
  - SPF & DKIM
  - Review Transport Rules
  - Basic Exchange Online Protection Policies
- Enable MS Defender AV best practices

Elevated

- Enable adv. mail security policies (Defender for O365)
  - Safe Attachment & link
  - Anti-phishing & Impersonation
- Enable Defender for Endpoints
- Enable Defender Credential guard
- Deploy CloudApp Security using SecWise best practices
  - Oauth App review
  - Govern discovered Apps
- Deploy MS Defender Identity using SecWise best practices
- Deploy Azure Sentinel using SecWise best practices

Advanced

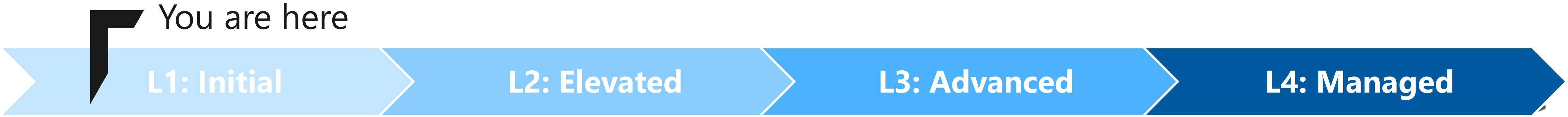
- Enable DMARC
- Enable Defender AV & for Endpoints on Servers
- Enable Attack Surface Reduction Rules (ASR)/ Exploit Guard
- Enable Controlled Folder Access
- Hardened Windows Defender Firewall
- Connect on premise security controls to CloudApp Security

SecWise Watch

- Monitoring Threat & impersonation alerts
- Monitor Automated Investigations
- Monitoring endpoint security posture

SecWise Care

- Change requests
- Security Questions/assistance



SecWise Protect prerequisites

Light

For organizations with only:

- Office 365 E1 or E3 customers
- No M365 or EMS bundle

GPO, SCCM or Intune

Elevated

- M365 E5

OR

- EMS E5

OR

- Security E5 add-on

OR

- M365 Education A5

AND

- Azure Subscription

Advanced

- Windows Enterprise
- > Windows Server 2016

SecWise Watch

- Azure Subscription
- Sentinel Implemented
- SecWise watch subscription
- At least SecWise Threat Elevated implemented

SecWise Care

- Care buckets or SecWise watch subscription een) -

Thank You

SecWise