

SEPAGO ADAPT



sepago. making people love it.

Neue Werkzeuge, neue Prozesse?

Die Arbeit mit der M365 Defender-Lösung erfordert eine Veränderung der Prozesse. Basierend auf unseren Erfahrungen aus früheren Kundenprojekten und den Best Practices von Microsoft wollen wir gemeinsam mit Ihnen Prozesse für Ihr Unternehmen entwickeln und etablieren, damit Sie alle Funktionen von M365 Defender voll nutzen können. Das Ziel der Konzeption und Definition der neuen Prozesse ist ein strukturierter "Incident Handling und Remediation" Prozess, sowie die perspektivische Implementierung in ein ITSM oder die Dokumentation in einem "Process Warehouse" für regulatorische Zwecke. Das volle Potenzial der eingesetzten technischen Sicherheitslösungen wird in diesem Modul ausgeschöpft.

Vorteile eines ganzheitlichen Ansatzes



Agenda



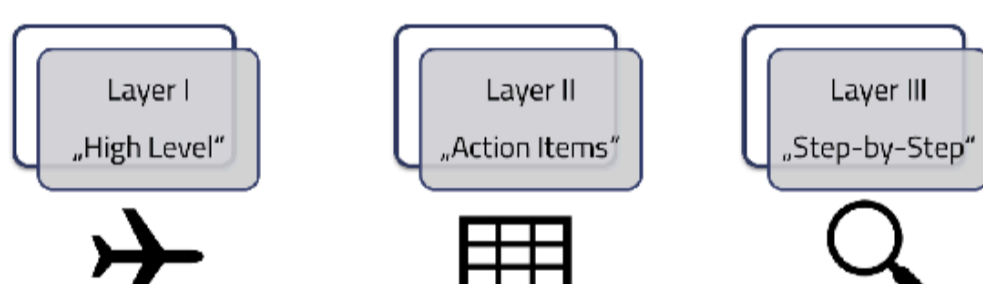
1. Kick-off
2. Stakeholder Analyse & Interviews
3. Umweltanalyse
4. Identifikation der Prozessauslöser
5. Prozess-Ebene 1 - Hig-Level (Visio Swimlane)
6. Leitfaden zur Prozesskommunikation
7. Prozess-Ebene 2 - Action Item (Excel Actions)
8. FTE Berechnung und Bedarf an Fähigkeiten/ Ressourcen
9. Handhabung & Leitfaden
10. Prozess Onboarding & Bewusstsein für IT-Sicherheitsprozesse
11. Prozessüberprüfung und -verbesserung

Nachdem wir Ihr Unternehmen in der Onboarding-Phase kennengelernt haben, beschreiben wir Ihre neuen M365 Defender-Prozesse in drei Stufen. Sepago adapt liefert die Erstellung, Dokumentation und Implementierung/Onboarding der folgenden Prozessebenen:

1. Prozess-Ebene 1 - High-Level (Visio Swimlane)
2. Prozess-Ebene 2 - Action Item (Excel Actions Items mit RACI-Zuordnung)
3. Prozess-Ebene 3 - Betriebshandbuch/Playbook-Dokumentation (PDF/Word als Wissensbasis)
4. Optional: ITSM-Implementierung & Prozessüberwachung (individuell)

Zunächst werden die Prozesse auf hoher Ebene und ein allgemeiner Überblick über die Arbeitsabläufe dargestellt, um die Prozessphasen und die Hauptverantwortlichen zu visualisieren. Als Nächstes wird jeder Arbeitsablauf von der ersten Ebene aus aufgeschlüsselt und die RACI-Matrix durchlaufen, um die Zuständigkeiten festzulegen und sicherzustellen, dass jeder zu jedem Zeitpunkt seine zugewiesenen Aufgaben kennt.

Die dritte Ebene besteht aus einem Schritt-für-Schritt-Handbuch, das von Ihren Sicherheitsanalysten für die tägliche Arbeit verwendet werden kann.



| | Layer I | Layer II | Layer III |
|------------|--|---|---|
| Zweck: | High-Level Überblick über Prozesse und Workstreams | Action Item Listen für jeden Workstream inkl RACI Matrix | Schritt-für-Schritt Dokumentation |
| Inhalt: | Prozessphasen, Start und Häufigkeit der einzelnen Prozesse, Abhängigkeiten, Hauptverantwortliche und Stakeholder | Wer ist für welches Action Item in welcher Reihenfolge verantwortlich, um die Workstreams zu erfüllen | Alle nötigen Details, wie die Action Items durchzuführen sind |
| Plattform: | Visio(s) | Excel | Word |

Change Management

Da neue Prozesse, insbesondere in Kombination mit neuen Lösungen, in Ihrer Organisation auf Widerstand stoßen können, bieten wir Ihnen ein umfassendes Widerstand in Ihrer Organisation hervorrufen können, bieten wir Ihnen ein umfassendes Änderungs- und Einführungsmanagement. Wir bieten eine Vielzahl von bewährten Techniken, um die beste Anpassung an Ihr Unternehmen zu gewährleisten. Die Kombination von Adoptions- und Änderungsmanagement mit der gemeinsamen Erstellung von Prozessen stellt sicher, dass Ihre neuen Microsoft Defender 365 -Lösungen den größten Nutzen für Sie erbringen können.

Herausforderungen und Risiken im Zusammenhang mit diesem Projekt können die folgenden sein und müssen während der Projektimplementierung und in regelmäßigen "weekly's" berücksichtigt und bewertet werden:

- Identifizierung der relevanten Prozessauslöser und der Sicherheitssystemlandschaft
- Standardisierung des "Incident Handling and Remediation" Prozesses
- Befragung & Onboarding der relevanten Stakeholder
- Organisatorisches Wachstum hin zu einer globalen Gruppe
- Klare & strukturierte Vorbereitung auf Majpr Incidents
- Kommunikation, Bedeutung und Team-Ressourcen der Security Operations Aktivitäten

Da sich die Bedrohungslandschaft ständig weiterentwickelt, müssen die Sicherheitsabläufe und -prozesse auf dem neuesten Stand gehalten werden. Um Sie bei dieser kontinuierlichen Aufgabe zu unterstützen, bieten wir Ihnen auch unseren Service zur kontinuierlichen Verbesserung auf monatlicher Basis an.

sepago adapt stellt sicher, dass Ihr Sicherheitsteam in der Lage ist, zu jedem Zeitpunkt die für Ihr Unternehmen passenden Prozesse zu befolgen. So wird sichergestellt, dass Lösungen wie M365 Defender ihr volles Potenzial entfalten und den Sicherheitsstatus Ihrer Organisation stärken können.



KONTAKTIEREN SIE UNS

ANJA KRUMKAMP
IT Security Sales

sales@sepago.de

sepago. making people love it.