sepago. making people love it.

New tools new processes?

Working with the M365 Defender solution requires a change in processes. Based on our experiences from previous customer projects and Microsoft best practices, together we will build and establish processes for your organisation to enable you to fully use all M365 Defender features. The purpose of the conception and definition of the new processes is a structured "incident handling and remediation" process, as well as perspective implementation in an ITSM or documentation in a "process warehouse" for regulatory purposes. The full potential of the technical security solutions used is leveraged in this module.

BENEFITS HOLISTIC APPROACH

Overview & foresight operations

Structured designed workflows

Build internal operation knowledge

Meet regulatory requirements

Clear interfaces with external partners

Constant development with automation

Agenda

1. Kick-off
2. Stakeholder Analyse & Interviews
3. Environment analysis
4. Process Trigger identification
5. Design Process Layer 1 - High
6. Process Communication guideline
7. Definition Process Layer 2 - Action Items
8. FTE calculation & skill/resource demand
9. Major incident handling & guideline
10. Process Onboarding & IT Security Process Awareness
11. Process Review & Improvement

After we get to know your organization during the onboarding phase, we describe your new M365 Defender processes in three levels. Sepago adapt delivers the creation, documentation and implementation/ onboarding of the following process levels:

1. Process layer 1 - High-level (Visio Swimlane)
2. Process layer 2 - Action item (Excel Actions Items with RACI allocation)
3. Process layer 3 - Operation manual/playbook documentation (PDF/Word as knowledge base)
4. Optional: ITSM Implementation & Process Monitoring (custom)

First, high level processes and a general workstream overview, to visualize the process phases and main responsible stakeholders. Next, we drill down each workstream from level one and move through the RACI matrix to define responsibilities, making sure that at each point in time everyone knows their assigned tasks.

The third level consists of a step-by-step operations manual, which can be used for everyday operations by your security analysts.
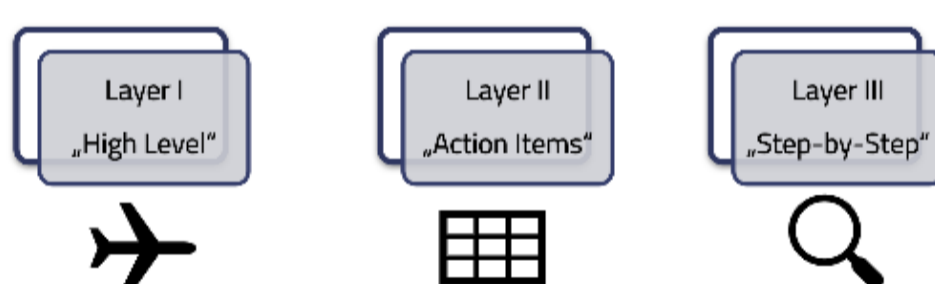
	Layer I	Layer II	Layer III
Purpose:	High level process & workstream overview	Action Item Lists for each workstream with RACI	step-by-step documentation
Informs about:	Process phases, process starts & frequencies, dependencies, main responsible stakeholder	Who needs to do which Action Items in which order to fulfill the workstreams	All needed details how to fulfill the Action Items
Assembeled in:	Visio(s)	Excel	Word

Change Management

As new processes, especially in combination with new solutions, can bring a certain amount of resistance from your organization, we offer you extensive change and adoption management. We offer a variety of proven techniques to ensure the best fit for your organization. Combining adoption and change management with joint process creation ensures that your new Microsoft Defender 365 solutions can bring the most value for you.

Challenges and risks related to this project may be the following and need to be considered and evaluated during project implementation and in periodic "weekly's":

- Identification of relevant process triggers & the security system landscape
- Standardization of the "incident handling and remediation process"
- Survey & Onboarding of relevant Stakeholders
- Organizational growth towards a global group
- Clear & structured preparation for "major incidents"
- Communication, importance & team resources of Security Operations activities

As the threat landscape is constantly evolving, security operations and processes have to be kept up to date. To support you in this ongoing task, we also offer our service for continuous improvement on monthly basis.

sepago adapt ensures that your security team is enabled to follow processes fitting your organization at each point in time. This makes sure that solutions like M365 Defender can unfold their full potential and fortify the safety status of your organization.

PLEASE CONTACT US

ANJA KRUMKAMP
IT Security Sales

sales@sepago.de

sepago. making people love it.