sepago adapt

Customer Case Study

SEPAGO IN A NUTSHELL

SYSTEM INTEGRATOR,
ISV AND CLOUD MANAGED
SERVICE PROVIDER

SINCE 2002

SUCCESSFUL ON THE MARKET
AT THREE LOCATIONS:
COLOGNE HAMBURG MUNICH

SPECIALISED IN

MICROSOFT CLOUD TECHNOLOGIES, MODERN WORKPLACE,
MOBILITY, APP VIRTUALISIERUNG & VDI, CITRIX WORKSPACE
APP, VIRTUAL MANAGED SERVICES AND IT-SECURITY

HUNDREDS OF SATISFIED CUSTOMERS

85 ENTHUSIASTIC EMPLOYEES

EXCELLENT ORGANIZATIONAL CULTURE
COMMUNITY AWARDS

MILLIONS OF GOOD IDEAS

THE COMPANY

- small, Germany-based manufacturing company (hidden champion)
- 12.500 employees generated about 2,5 billion € in 2019

Current Challenge:

Customer will introduce Microsoft Endpoint Management. But the Security Operations Team is not operationally structured yet and does not know how to integrate the software into the existing IT landscape and how to operate the security solutions.

CUSTOMER PROBLEM & CURRENT SITUATION

- New Microsoft Security tools require new processes
- General workstream overview required
- Allocated Action Items through RACI matrix
- Step-by-step documentation for upskilling
- Forecast FTE ressources

WHAT WE DELIVERED

- Identification of relevant process triggers & the security system landscape
- Integration of Microsoft Endpoint Management into the existing IT 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

AGENDA OF THE ENGAGEMENT

Design Process level 1 high level

- high level process description
- description key use cases based on Change phases

Define process level 2 action item

- Definition roles, interfaces & RACI allocation
- action-item definition

Document process level 3 step-by-step

- step-by-step documentation (operational manual)
- onboarding documentation
- methods and tools documentation (toolkit)

Optional: Establish process monitoring

- Establishing a measurement plan (technical & UX/IT Stakeholder feedback)
- Establishing a Power BI based measurement dashboard
- Establishing and documenting the measurement process
- Appropriate actions and improvements based on the measurement results

Optional: Implementation in ITSM

- Visualizing the process
- Organizing the workflows
- Documenting the workflows
- Automizing the workflow
- Established KPI-Source for measurement/monitoring

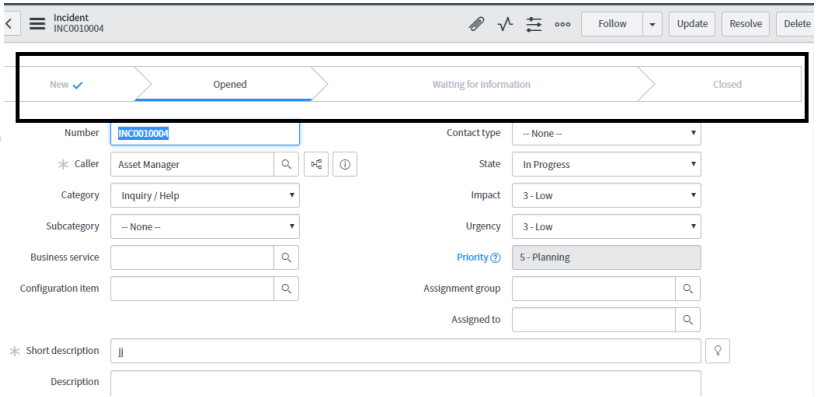
PROCESS ARCHITECTURE & EXAMPLES

„BEGIN WITH THE END IN MIND“

One source of documentation (operational manual/process)

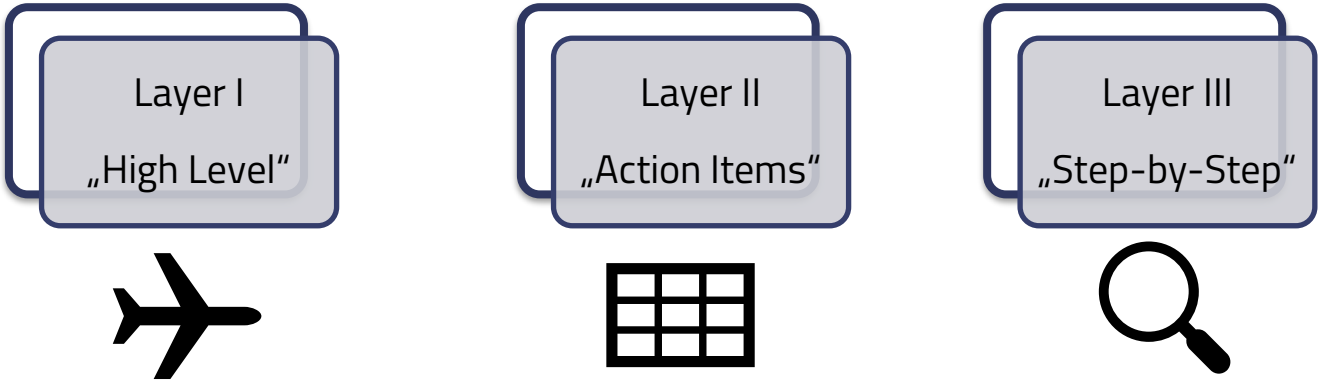
The process documentation is transferred to your ITSM (e.q. Service Now)

- ✓Visualizing the process
- ✓Organizing the workflows
- ✓Documenting the workflows
- ✓KPI-Source for measurement/monitoring



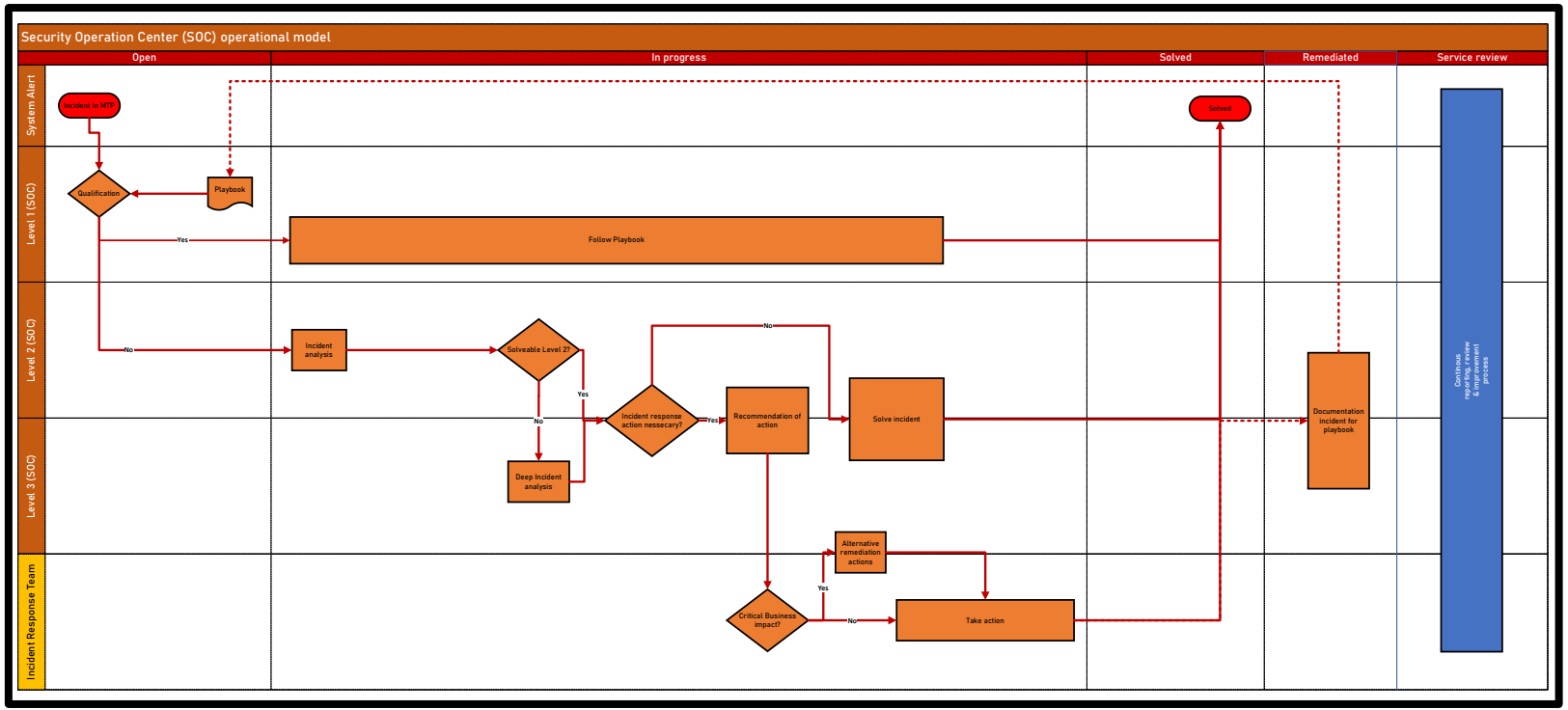
servicenow™

PROCESS STRUCTURE



	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

EXAMPLE LAYER I – HIGH LEVEL



EXAMPLE LAYER II – ACTION ITEMS

Workstream Constitutional - Action Items	Median time/Incident	LVL1	LVL2	LVL3	SecSME	SocTL	SDM	SecEng	IR	SME	CISO
Phase: Open											
Incident in MDATP	0										
Check incident monitoring automation		R				A		C			
Monitor incident queue		R				A					
Decision: Qualification	10										
Assign incident to relevant Analyst		R	C			A					
Check for existing documentation in playbook		R	C			A					
If existing documentation in playbook: Follow-playbook		R	C			A					
If not existing documentation in playbook: Fill ticket template: Incident analysis		R	I			A					
Phase: In progress											
Follow-playbook (if existing documentation in playbook)	5										
Open playbook		R				A					
Search for incident category		R	C			A					
Follow playbook instructions		R	C			A					

EXAMPLE LAYER III – STEP BY STEP (RUNBOOKS)

Workstream	Feature Review process
Action Item	Prepare environment for testing new features
Predecessor	Decide which features should be implemented
Accountable	PO WIN
Responsible	OPS WIN
Consultable	OPS MECM, PO WIN, PO SEC, OPS AD, ITSEC
To Inform	EPO, PO MECM, OPS AD
Start trigger	Action Item "Decide which features should be implemented" completed.

1. Short description of Action Item

This Action Item is done to ensure that the test environment fulfills all requirements to do the testing.

2. How to fulfill Action Item

a) Open the corresponding feature review document in Evergreen IT Teams under *Waas > Files > TechDocs > 1909 1903 Feature overview and decision table.xlsx*

b) Check the column "FRB approved for test". For each feature that FRB approved, prepare any depended recourses that are required to run a test of this feature, things like:

   a. ADMX template import if you can't test the functionality by using local group policies.
   b. Prepare test devices with the target Windows 10 version installed.
   c. Prepare a server that hosts the new feature that needs to be tested.

3.19 Malware

3.19.1 'Mimikatz' hacktool was detected	
Severity:	High
Detection Source:	AntiVirus
Detection Status:	Prevented

Analysis:

I. Understand the threat
   A. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=HackTool%3aWin32%2fMimikatz.D

II. Check the timeline
   A. Was the file "remediated successfully"
      ⇨ Threat got remediated by „Automatic Remediation"
      ⇨ Check the Audit Logs oft he „Automatic Remediation" for details

Remediation:

Already remediated by "Automatic Remediation"

OUTCOME FOR THE CUSTOMER

Overview & foresight operations

Structured designed workflows

Build internal operation knowledge

Meet regulatory requirements

Clear interfaces with external partners

Constant development with automation

„Matching organization & tool knowledge for successful operations“

THANK YOU FOR YOUR ATTENTION!

Let us hear from you!