Use case diagrams

UC_00 - Initialization and configuration of SOCaaS

Figure 2 : UC_00 - Initialization and configuration of SOCaaS

Use case	UC_00 - Initialization and configuration of SOCaaS
Goal	The use case describes the initial initialization and setup of SOCaaS for a new customer. It includes the activation of logging sources, the configuration of integration points, dashboards and basic security processes.

Precondition	The customer has a tenant created.
Precondition	The Architect has configuration permissions.
Precondition	
Postcondition	SOCaaS is successfully initialized and ready for monitoring and detection.
Postcondition	The basic modules are activated: logging, SIEM correlations, dashboards, incident management.
Postcondition	Logs from all mandatory sources contain the mandatory fields for detection.
Basic Path	Basic Path
Step	**Activity**
1	The architect starts the initialization process for a new customer.
2	The system loads the customer profile and prepares the configuration interface.
3	
4	The system performs initialization tasks (source registration, agent activation, dashboard creation).
5	The architect confirms the configuration.
6	The system saves the configuration and reports successful completion.
ALT_00_01 – Incomplete customer profile	Alternate
Step	**Activity**
1	The system detects missing data.
2	It notifies the architect to supply the missing data.
3	The process continues once the information has been supplemented.
ALT_00_02 – Unavailable logging sources / infra	Alternate
Step	**Activity**
1	
2	
3	The process continues with limited functionality.
Use case	UC_00a - Verification of the customer profile
Goal	The system verifies whether the customer tenant contains all mandatory data (identification, technical, integration).

Precondition	The tenant exists in the system.
Postcondition	The customer profile is confirmed as complete.
Basic Path	Basic Path

Step	**Activity**
1	The platform operator starts the profile verification.
2	The system loads the customer data.
3	The system checks the mandatory fields.
4	The verification is successful.
ALT_00a_01 – Incomplete data	Alternate
Step	**Activity**
1	The system requests that the missing data be supplied
ALT_00a_02 – The tenant lacks technical configuration	Alternate
Step	**Activity**
1	The system stops the process and notifies the administrator.
Linked functional requirements	
FREQ_021 - Onboarding of a new customer	SOCaaS. This includes: • setting up the logging agent • configuration of correlation rules • creation of separated dashboards • setting up incident management for the customer
Use case	UC_00b – Activation of logging agents
Goal	The system activates the customer's logging agents to send logs to SOCaaS.

Precondition	The customer systems are available.
Precondition	Communication channels are open.
Postcondition	The logging agents are active and sending data.
Basic Path	Basic Path
Step	**Activity**
1	The platform operator starts the activation.
2	The system contacts the logging agents.
3	
4	The agents are activated.
ALT_00b_01 – The agent does not respond	Alternate
Step	**Activity**
1	The system reports an error and continues later.
ALT_00b_02 – Invalid API keys	Alternate
Step	**Activity**
1	The system requests the keys to be uploaded again.
Linked functional requirements	
FREQ_008 - Log centralization	

Use case	UC_00c – Setting up correlations and dashboards
Goal	The system creates predefined correlation rules and dashboards for monitoring security events.

Precondition	The SIEM module is active.
Precondition	Logs are arriving in the system.
Postcondition	Correlation rules and dashboards are configured.
Basic Path	Basic Path
Step	**Activity**
1	The platform operator starts the setup.
2	The system loads the correlation template.
3	The system creates dashboards for monitoring.
4	The configuration is saved.
ALT_00c_02 –	Alternate
Step	**Activity**
1	The system creates only a minimal version. (the last executable one)
ALT_00c_01 – The correlation rule is invalid	Alternate
Step	**Activity**
1	The system skips it and reports an error.
Linked functional requirements	
FREQ_001 - Security event monitoring process	– ensures the collection and tracking of logs, metric data and alerts from all integrated systems.
FREQ_006 - Reporting and visualization process	– ensures regular output for management, auditors and SOC analysts.
Use case	UC_00d – Setting up incident management
Goal	The system activates the workflow for incident management and role assignment.

Precondition	The Ticketing or SOAR module is initialized.
Postcondition	The incident lifecycle (triage → analysis → closure) is ready.
Basic Path	Basic Path
Step	**Activity**
1	The platform operator starts the configuration.
2	The system loads the workflow templates.
3	The system creates incident categories and priorities.
4	It assigns roles (Analyst, Operator, Manager).
ALT_00d_01 – User roles do not exist	Alternate
Step	**Activity**
1	The system stops the workflow and asks the administrator to add roles.
ALT_00d_02 – The Ticketing module is unavailable	Alternate

Step	**Activity**
1	The system activates only the basic SOAR fallback.
Linked functional requirements	
FREQ_004 - Incident management process	– includes the recording, classification, priority assignment, documentation and closure of incidents.

Figure Diagram Sequence : UC_01 - Monitor security events

Use case	
Goal	The use case describes the continuous monitoring of security events within SOCaaS. It includes event collection, their normalization, enrichment and the preparation of alerts for the subsequent incident detection process.

Precondition	The logging agents are active.
Precondition	The SOCaaS SIEM module is functional.
Precondition	UC_00 (initialization) has been successfully completed.
Postcondition	The events are processed and passed on to the incident detection process.
Postcondition	The alerts are displayed to the operator.
Postcondition	Monitoring runs in real time.
Basic Path	Basic Path
Step	**Activity**
1	The operator monitors the control dashboard in SOCaaS.
2	UC_01a: The system receives events from logging sources.
3	UC_01b: The system normalizes and enriches the data.
4	UC_01c: The system indexes the stored data for fast searching.
5	SOCaaS generates alerts based on correlation rules.
6	The operator sees the resulting security events.
7	The use case ends; monitoring continues without restriction. The operator evaluates the alert.
8	If it is critical →
9	The Use Case ends – monitoring continues.
ALT_01_01 – Unavailable logs or agents	Exception
Step	**Activity**
1	SOCaaS is not receiving data from the source.
2	The system creates a “Missing logs” alert.
3	
ALT_01_02 –	Exception
Step	**Activity**
1	
2	The system enables protective mechanisms (rate-limiting, buffering).
3	The operator is notified of the risk of event loss.
Linked functional requirements	
FREQ_001 -	– ensures the collection and tracking of logs, metric data and alerts from all integrated systems.

Security event monitoring process	
Use case	UC_01a - Log collection
Goal	It ensures the technical reception of logging data from systems, applications, devices and sources into the SIEM platform. It is the foundation of the monitoring process.

Precondition	The communication channel between the system and the agent is functional.
Precondition	The logging agent is active.
Postcondition	The logs are ready for the next step – normalization.
Postcondition	SOCaaS has received new logs.
Basic Path	Basic Path
Step	**Activity**
1	The logging agent sends security events.
2	SOCaaS receives the data.
3	The format and integrity of the logs are verified.
4	The logs are passed on to the normalization process.
ALT_01a_01 – Logs are not delivered	Alternate
Step	**Activity**
1	SOCaaS does not record any data from the source.
2	The system creates a “Missing logs” notification.
3	The administrator receives a notification.
ALT_01a_02 – Invalid log format	Alternate
Step	**Activity**
1	The log has an incorrect format or missing fields.
2	SOCaaS rejects it and stores it in the quarantine buffer.
3	A notification is sent to the integrator.
Linked functional requirements	
FREQ_008 - Log centralization	
Use case	UC_01b – Data normalization and enrichment
Goal	The use case ensures the normalization of logs into a unified format and their enrichment with information from CTI, the asset database or user data.

Precondition	A configuration of normalization rules exists.
Precondition	UC_01a (log collection) was successful.
Postcondition	The log is normalized and enriched.
Postcondition	The data are ready for storage and indexing.
Basic Path	Basic Path
Step	**Activity**
1	SOCaaS loads the received logs.
2	A normalization profile is applied according to the source type.
3	Data enrichment (IP reputation, hostname, user).
4	The resulting event is ready for indexing.
ALT_01a_01 – Unknown log type	Alternate

Step	**Activity**
1	The system uses a fallback normalization profile.
ALT_01a_02 – CTI feed is missing	Alternate
Step	**Activity**
1	The system performs normalization without enrichment and marks the event as “unenriched”.
Linked functional requirements	
FREQ_009 - Data normalization and enrichment	
Use case	UC_01c – Data indexing and storage
Goal	The use case handles the storage of normalized security events in storage and their indexing for fast searching and correlation mechanisms.

Precondition	Data normalization (UC_01b) is completed.
Precondition	The storage and the cluster are available.
Postcondition	The events are stored in the SIEM database.
Postcondition	The indexes are ready for query systems.
Basic Path	Basic Path
Step	**Activity**
1	The system takes over the normalized data.
2	It writes them to storage (DB or distrib. index).
3	It creates/updates the indexes.
4	The event is available for correlation rules.
ALT_01c_01 – Storage unavailable	Alternate
Step	**Activity**
1	The system stores the data in a buffer and creates an alert.
ALT_01c_02 – Exhaustion of storage space	Alternate
Step	**Activity**
1	The system activates a clean-up or alerts operations.
Linked functional requirements	
FREQ_010 - Data storage and indexing	

Figure Diagram Sequence : UC_02 - Visualize and report security data

Use case	UC_02 –
Goal	The system enables SOC operators and the administrator to display security events using

	dashboards, filters, charts and tabular outputs. It also enables report generation and data export for management, audit or customers.

Precondition	The dashboards are defined in the configuration (UC_00c).
Precondition	UC_01c – The data are indexed and available for visualization.
Precondition	UC_01 – Monitoring is running and providing data.
Postcondition	The activity is recorded in the audit log.
Postcondition	The report has been generated or exported (if initiated).
Postcondition	The user sees updated visualizations.
Basic Path	Basic Path
Step	**Activity**
1	The actor opens the “Visualization and reporting” module.
2	The system loads the available dashboards and reports according to the actor's role.
3	The actor opens a dashboard → the system displays charts, metrics, tables.
4	
5	
6	The system compiles the report according to the selected format and template.
7	
ALT_02_01 – Unavailable data	Alternate
Step	**Activity**
1	The dashboard returns an empty dataset.
2	The system displays a warning.
3	
ALT_02_02 – Incorrect permissions	Alternate
Step	**Activity**
1	An actor (e.g. the Operator) opens a dashboard outside their tenant.
2	The system displays the error “Insufficient permissions”.
ALT_02_03 – Report generation failed	Alternate
Step	**Activity**
1	It displays an error message.
2	It saves the error in the audit log.
3	An actor (e.g. the Operator) opens a dashboard outside their tenant.
Linked functional requirements	
FREQ_006 - Reporting and visualization process	– ensures regular output for management, auditors and SOC analysts.
Use case	UC_02a –
Goal	The user opens a dashboard that visualizes security events, metrics and system states in real time.

Precondition	The system is initialized and configured (UC_00).
Precondition	All log sources are active and data are being received (UC_01).
Precondition	The user is authenticated and has a role that allows dashboards to be displayed.
Postcondition	The dashboard has been displayed with current data.

Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The actor opens the Dashboards module.
2	The system loads the available dashboards according to the role.
3	The actor selects a dashboard to display.
4	The system loads and renders the visualizations (charts, heatmaps, tables).
5	The system updates the visualizations in real time or at defined intervals.
ALT_02a_02 – The user does not have permission for a specific dashboard	Alternate
Step	**Activity**
1	The system hides the dashboard or displays “Access Denied”.
2	
ALT_02a_01 – Data do not load	Alternate
Step	**Activity**
1	
2	Instead of charts, it displays the message: “Data are not available.”
3	
Linked functional requirements	
FREQ_012 - Visualization of outputs	
FREQ_032 - Dashboard structure	ables, heatmaps, distribution histograms, metrics or maps. Each dashboard within SOCaaS is designed as a composition of these visualizations focused on a specific aspect of monitoring or analysis. System security overview Correlation and incident dashboards Monitoring of authentications and user behaviour Integrated overview for the SOC analyst
FREQ_031 - Dashboard design	layers as follows: 1. Global overviews (SOC Overview) Intended for management and SLA reporting – they include daily/monthly incident statistics, threat types, top 10 IP addresses, countries of origin of attacks, ticket resolution time. 2. Alert monitoring dashboards Focused on operational monitoring – they display new alerts, breakdown by severity (Critical, High, Medium), time trends, and correlations between multiple sources. 3. Thematic dashboards They cover specific areas: • EDR activities: recorded files, processes, attempts to execute malicious code. • Vulnerabilities and scans: results from Greenbone or OpenSCAP. • 4. Detailed analytical dashboards – Used by L2 analysts and for threat hunting. They contain heatmaps, time slices, distributions by hour, country, ASN, IOC occurrence and the like. 5. Ad-hoc and incident-specific dashboards – Created during the investigation of a specific case, where the analyst builds their own visualization based on data from Elasticsearch.
Use case	UC_02b –
Goal	The user creates a one-off report or saves a reporting template based on data from dashboards or events.

Precondition	The dashboards are available and the data are indexed (UC_01).
Precondition	The user has the “Create Report” permission.
Postcondition	The report is saved in the system.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The actor opens the Reports module.
2	
3	Selects: report type, time range, template or custom design.
4	The system loads the necessary data.
5	The user confirms the generation.
6	The system generates the report and saves it in the report database.
ALT_02b_02 – Unavailable data for the report	Alternate
Step	**Activity**
1	The system displays the message “Data for the selected period are not available”.
2	The Operator, the Platform Operator or the Administrator selects a different period.
ALT_02b_01 – Invalid report parameter	Alternate
Step	**Activity**
1	The system detects a missing parameter (time period, data source...).
2	It displays an error and requests that it be supplied.
Linked functional requirements	
FREQ_033 - Reporting	• Operational overview – display of system status, number of incidents, agent activity. • Security reporting – outputs on detected threats, attack types, trends. • Compliance reporting – reports according to regulatory requirements (e.g. GDPR, NIS2). • Management reporting – aggregated statistics and indicators for the organization's leadership. • Customer reporting – individual overviews for individual clients of the multi-tenant SOCaaS.
Use case	UC_02c –
Goal	The user exports an existing report to PDF, CSV, JSON or PNG and can send it by email or webhook.

Precondition	There is a generated report (UC_02b).
Precondition	The user has “Export Report” rights.
Postcondition	The system has created a file in the selected format.
Postcondition	The file has been downloaded or sent to an external endpoint.
Basic Path	Basic Path
Step	**Activity**
1	The user opens the report detail.
2	
3	Selects the format (PDF/CSV/JSON/PNG).
4	The system generates the export.
5	The file is downloaded or sent according to the settings.
	Alternate

ALT_02c_02 – Insufficient permissions	
Step	**Activity**
1	The system displays “Access Denied”.
2	
ALT_02c_01 – Export fails (timeout, large dataset)	Alternate
Step	**Activity**
1	The system reports an export error.
2	It offers an offline export or splitting of the data.
Linked functional requirements	
FREQ_034 - Manual export of reports	• PDF document – a generated snapshot of the current dashboard. • PNG image – static images of individual visualizations. • CSV files – raw data from tables and data fields. • JSON – for automated analysis and further processing.
FREQ_165 - Support for export to PDF, CSV, JSON	
	-mail, webhook)

Figure Diagram Sequence : UC_03 - Manage detection and correlation rules

Use case	
Goal	This use case covers the activities of analysts and administrators in creating, managing and maintaining detection and correlation rules in the SOCaaS environment. These rules enable the detection of security threats based on IOCs, behavioural anomalies, event chaining or threshold values. The use case focuses exclusively on the rule management process – their definition, tuning, classification and mapping to security frameworks (e.g. MITRE ATT&CK).

Precondition	The actors have access to the administration interface for creating rules.
Precondition	The system supports the definition, management and versioning of detection rules.
Postcondition	A new rule is created or an existing rule is modified, deactivated or deleted.
Postcondition	The rule is versioned, validated and ready for deployment to the production environment.
Postcondition	The rule is available for evaluating security events (UC_04).
Basic Path	Basic Path
Step	**Activity**
1	The analyst or administrator opens the interface for managing detection rules.
2	Creates a new rule or searches for an existing one.
3	Defines the conditions: event type, IOC/indicator, frequency of occurrence,

	source/destination entities,
4	
5	The rule is saved and versioned.
6	
7	
ALT_03_01 – The rule is tested on historical data (debugging)	Alternate
Step	**Activity**
1	The analyst uses a tool to test rules against historical logs.
2	The results are displayed; the rule is then modified or approved.
ALT_03_02 – The rule is created via a no-code interface	Alternate
Step	**Activity**
1	The analyst uses a visual interface (drag & drop) to create conditions without writing syntax.
2	The platform automatically generates the underlying code of the rule.
Linked functional requirements	
FREQ_029 - Correlation rules and threat detection	• Alerts on basic IOCs – comparison against a database of known indicators (IP, URL, hash). • Anomalous user behaviour – e.g. multiple failed logins within a short time, login from a new geographical region. •– e.g. DNS queries to dynamically generated domains (DGA), deviations in time and data volume. • Activities with administrative privileges – e.g. adding a user to the “Administrators” group, ACL changes, running netsh, powershell. •– correlation between multiple logs over time: e.g. login ? file transfer ? execution of a malicious process. These rules will be managed in a way that makes it possible to: • • • •objects.
FREQ_045 - Custom alerting rules and thresholds	
FREQ_041 - Event correlation	
FREQ_050 - Support for MITRE ATT&CK mapping	
FREQ_011 - Creation of correlation rules	

UC_04 –

Figure Diagram Sequence : UC_04 – Notify and escalate a security incident

Use case	UC_04 –
Goal	After the system detects and creates a security incident (UC_01, UC_03), the objective of UC_04 is to ensure that the right person (1st level) learns about it in time, that someone takes over the incident and that, in the event of inactivity or a worsening of severity, the incident is automatically moved to a higher level

Precondition	There is an incident –
Precondition	Notification and escalation policies are set up

Precondition	The contact channels and the on-call schedule are known
Postcondition	The relevant recipient has been notified
Postcondition	The incident has a recorded history of notifications/escalations
Postcondition	In the event of inactivity, escalation has taken place according to the SLA
Basic Path	Basic Path
Step	**Activity**
1	Creation or change of an incident
2	Evaluation of the notification policy
3	Selection of primary recipients
4	Generation of the notification message
5	Sending of the notification via primary channels
6	Waiting for confirmation (acknowledgement)
7	Acknowledgement of the incident by the Analyst/Operator
8	Stopping further escalation
9	Update of the incident history
ALT_01 – Failure of the primary notification channel	Alternate
Step	**Activity**
1	Sending the notification fails (e.g. the e-mail server is unavailable).
2	The system automatically tries an alternative channel (e.g. SMS, another mail gateway, chat).
3	Both the unsuccessful attempt and the subsequent fallback are recorded in the incident history.
4	If all channels fail, the incident is flagged “notification unsuccessful” and the system automatically creates an internal ticket for the infrastructure administrator.
ALT_02 - The incident is not acknowledged within the SLA time - escalation	Alternate
Step	**Activity**
1	After the SLA interval has elapsed, the incident has not been acknowledged.
2	The system automatically escalates the incident to a higher level (Manager, SOC Lead): increasing the priority / severity of the incident, sending an escalation notification to the Manager via their preferred channels.
3	A record of the failure to take over within the SLA and of the escalation performed is added to the incident history.
4	Optionally, a further playbook is launched (e.g. partial automated measures, pre-prepared actions).
Linked functional requirements	
	and incident tickets
FREQ_128 - Notifications of status changes, expirations, service intervals	Automatic notifications upon a change of status or the need for service intervention. Alerts on status changes, expirations, service intervals
FREQ_056 - Incident categorization and prioritization	
FREQ_015 - Ticketing system and incident management	tracking of the resolution.
FREQ_003 - Incident response process	– defines the way in which the team responds to identified incidents. It includes escalation, assignment of responsibility, implementation of measures, as well as communication with the affected parties.

UC_05 –

Figure Diagram Sequence : UC_05 – Resolve and close a security incident

Use case	UC_05 –
Goal	After the incident has been detected and notifications have been sent (UC_01, UC_03, UC_04), this UC covers the entire incident resolution process – from takeover, analysis and implementation of corrective measures to the closure of the incident and complete documentation of its course (timeline, evidence, linked cases). The result is an incident that has a clear owner, implemented steps, recorded times and prepared materials for any “lessons learned”

Precondition	The incident has been created and notified
Precondition	The incident has an assigned owner / team
Precondition	Relevant data and logs are available
Postcondition	The incident has a documented course and outcome
Postcondition	The agreed set of corrective measures has been carried out
Postcondition	The incident is closed or reclassified
Basic Path	Basic Path
Step	**Activity**
1	Takeover of the incident by the Analyst
2	Collection and supplementing of evidence
3	Analysis and identification of causes
4	Proposal of corrective measures
5	Implementation of measures by the Administrator
6	Tracking of resolution times and progress
7	Review and approval of the outcome
8	Closure of the incident
9	Preparation of materials for lessons learned
ALT_ 01 – The incident is evaluated as a false positive	Alternate
Step	**Activity**
1	After the analysis, the Analyst finds that no incident occurred (incorrect correlation, test traffic).
2	The analyst updates the incident to the “false positive” status and briefly documents the reason.
3	The incident is closed but remains in the history, including the evidence –
ALT_02 –	Alternate
Step	**Activity**
1	The Administrator finds that the proposed measure has a high impact on operations (e.g. shutting down a critical service).
2	
3	The incident remains in the status “open – awaiting planned measures” with recorded times and risk.
Use case	UC_05a –
Goal	The analyst examines the incident in detail – reviews the timeline of events, logs and IOCs, adds evidence and builds a comprehensive picture of the cause and scope of the incident.

Precondition	The incident has been created and assigned to the Analyst.
Precondition	Basic logs and events from the monitoring system are available for the incident.
Postcondition	The incident contains supplementary evidence (logs, attachments, IOCs).

Postcondition	The preliminary cause of the incident and the extent of the impact are described.
Basic Path	Basic Path
Step	**Activity**
1	The Analyst opens the incident detail.
2	Displays the timeline of related events and logs.
3	Identifies suspicious events and indicators of compromise.
4	Downloads or requests additional logs/attachments and attaches them to the incident.
5	Based on the collected data, describes the preliminary cause and scope of the incident.
6	Updates the incident priority if necessary.
ALT_01 – Unavailable or incomplete logs	Alternate
Step	**Activity**
1	The analyst finds that logs are incomplete or missing; creates a task in the incident for the Administrator to remedy this (completing the logging, export from the source system) and continues working with what is available.
ALT_02 – The incident turns out to be a false positive	Alternate
Step	**Activity**
1	After the analysis, the analyst concludes that it is not a real incident; marks the incident as “false positive”, briefly documents the reason and UC_05 ends.
Linked functional requirements	
FREQ_133 - Adding attachments	ov)
	ion, closure)
Use case	UC_05b –
Goal	The Analyst and the Administrator create, assign and track tasks that represent specific corrective or preventive measures related to the incident.

Precondition	A basic analysis exists for the incident (UC_05a).
Precondition	It is clear which systems or services the incident affects.
Postcondition	The incident has a created list of tasks with assigned responsible persons and deadlines.
Postcondition	The status of individual tasks reflects the actual progress of handling (planned, in progress, done).
Basic Path	Basic Path
Step	**Activity**
1	Based on the analysis, the Analyst proposes specific corrective measures.
2	In the incident, creates tasks and assigns them to specific Administrators or teams.
3	Sets the priority and deadline for each task.
4	Administrators continuously update the status of tasks according to the implementation of measures.
5	The system records the times of creation, start and completion of tasks.
6	The analyst monitors the status of tasks and, as needed, sends reminders about or escalates delayed tasks.
7	After the key tasks have been completed, the Analyst

	updates the status of the incident.
ALT_01 – The task has a high impact on operations	Alternate
Step	**Activity**
1	rejects with a comment.
ALT_02 – The task cannot be implemented by the planned deadline	Alternate
Step	**Activity**
1	The Administrator updates the deadline and the reason in the task; the Analyst adjusts the incident priority as needed or informs the Manager.
Linked functional requirements	
FREQ_144 - Creation and management of cases - cases with tasks and details	
Use case	UC_05c –
Goal	After the corrective measures have been carried out, the Analyst (or the Manager) decides on the final status of the incident, documents the conclusion and links the incident with other related cases.

Precondition	The key tasks of the incident have been completed or a decision has been made to accept the remaining risk.
Precondition	Monitoring shows no persisting indicators of attack, or their occurrence has been explained.
Postcondition	
Postcondition	The incident is linked to other relevant incidents/cases or campaigns, if any exist.
Basic Path	Basic Path
Step	**Activity**
1	The analyst checks that all important tasks have been completed and the systems are stable.
2	Verifies in monitoring that no new related events are appearing.
3	
4	Fills in the final summary: cause, impact, measures taken.
5	Sets the final status of the incident (e.g. “closed”).
6	For critical incidents, asks the Manager to approve the closure.
7	The incident is moved to the archive and is ready for the “lessons learned” process.
ALT_01 – New related events detected during closure	Alternate
Step	**Activity**
1	b.
ALT_02 –	Alternate
Step	**Activity**
1	The analyst identifies that the incident belongs to a larger campaign; sets it as a child of the parent case and adjusts the final summary.
Linked functional requirements	
FREQ_146 - Linking cases based on common indicators	Automatic or manual identification of related incidents. Linking cases based on common indicators

UC_06 –

Figure Diagram Sequence : UC_06 – Evaluate incidents and improve detection and awareness

Use case	UC_06 –
Goal	After the incident has been resolved and closed (UC_05), this UC ensures that both the system and people learn from the incident: the incident is reviewed (post-incident / post-mortem), the findings are reflected in adjustments to detection rules and ML models, training / guidance for employees is prepared or updated.

Precondition	The incident is closed
Precondition	Data on the incident are available
Precondition	At least a basic “lessons learned” process exists
Postcondition	The incident has a processed “lessons learned” record
Postcondition	Adjustments to detection/ML have been proposed or carried out
Postcondition	Training / guidance for users has been prepared or updated
Basic Path	Basic Path
Step	**Activity**
1	Selection of incidents for evaluation
2	Preparation of supporting materials for evaluation
3	Post-incident meeting / review
4	Recording of lessons learned and recommendations
5	Proposal of adjustments to detection and ML models
6	model in the case of anomalies) and includes these findings in the proposed changes.
7	The knowledge base entry is linked to a specific incident (or attack type) so that it can be quickly
8	The outputs are stored in the knowledge portal / knowledge base and communicated to the relevant people.
9	Approval and planning of the deployment of changes
10	Preparation of training / awareness materials
11	Dissemination of knowledge
12	Conclusion of the UC
ALT_01 – Insufficient data for a quality evaluation	Alternate
Step	**Activity**
1	The analysis reveals that not all necessary logs or historical data are available; the team carries out basic lessons learned but at the same time creates tasks to improve logging and data collection in the future.
ALT_02 – The proposed adjustments to detection/ML are rejected	Alternate
Step	**Activity**
1	The Data Scientist or Developer prepares a proposal for changes, but the Manager does not approve them on the basis of risks or costs; the recommendations are stored in the knowledge base and the changes may be reconsidered

	later.
ALT_03 – A need for targeted employee training has been identified	Alternate
Step	**Activity**
1	training, which is assigned to a selected group of users.
Linked functional requirements	
FREQ_016 - Knowledge portal	ov.
FREQ_176 - Linking KB entries with specific incidents or attack types	specific incidents or attack types
FREQ_007 - Knowledge management process	– ensures the maintenance of the knowledge base of playbooks, documentation and recommended responses.
	regardless of class. Evaluation of the overall accuracy using metrics such as Precision, Recall, F1-score or AUC-ROC.
FREQ_026 - Creation of the knowledge base	• incident summary + lessons learned • entry in the knowledge portal • categorization according to MITRE ATT&CK and dates

UC_07 –

Figure Diagram Sequence : UC_07 – Automate incident response

Use case	UC_07 –
Goal	UC_07 addresses the situation when an incident has already been detected and is being handled (UC_05), but instead of purely manual steps, automated or semi-automated playbooks are used. Based on the incident type and TTPs, the system proposes suitable playbooks, orchestrates technical interventions (blocking, isolation, account disabling, ticketing) and records everything for audit purposes.

Precondition	The incident is in the “in progress” status
Precondition	Playbooks are available for the given incident type
Precondition	Integrations with the target systems are functional
Postcondition	The selected playbooks have been executed (auto / semi-auto)
Postcondition	All automated interventions are recorded in the incident for audit purposes
Postcondition	The incident is in a status that reflects the outcome of the automated response
Basic Path	Basic Path
Step	**Activity**
1	The analyst opens an incident in the “in progress” state and the system displays a list of proposed playbooks according to the incident type and the techniques used.
2	The Analyst selects a suitable playbook and chooses the execution mode (e.g. simulation, semi-automatic mode, fully automatic at low risk).
3	The system displays an overview of the planned playbook steps (e.g. IP block, endpoint isolation, account disabling, ticket creation).
4	In semi-automatic mode, before executing each step, the system requests the Analyst to confirm or skip the step.
5	The system gradually executes the approved steps via integrations with the target systems and continuously

	records the status (success/failure).
6	After the playbook finishes, the system summarizes the result: which actions were successful, what failed and where manual intervention is needed.
7	
8	Based on the result, the Analyst updates the incident status (e.g. containment done, awaiting monitoring, awaiting further tasks according to UC_05).
9	The incident continues in UC_05 (detailed analysis, addition of tasks, closure).
ALT_01 – No suitable playbook was found	Alternate
Step	**Activity**
1	_05 and marks the incident as a candidate for creating a new playbook in the future.
ALT_02 – A critical playbook step fails	Alternate
Step	**Activity**
1	An error occurs while an automated step is being executed (e.g. blocking on the firewall); the system marks the step as unsuccessful, records the error details and the Analyst decides whether to repeat the step, replace it with another measure or assign a manual task to the Administrator.
ALT_03 – The playbook runs only in simulation mode	Alternate
Step	**Activity**
1	Based on the Manager's policy, selected playbooks are permitted only in simulation mode; the Analyst runs a simulation, the system displays which actions would be performed and what the impact would be, and only then does the Analyst decide which of them will be performed manually or by means of partial automation.
Linked functional requirements	
FREQ_038 - Support for orchestration and automation	scaling of services, automated deployment of environments, repeatable testing and recovery from outages. In a SOC environment, where requirements and network topology change frequently, orchestration is essential to ensure flexibility, sustainability and operational efficiency.
FREQ_046 - Automated responses	SOAR)
FREQ_061 - Automated responses: IP block, host isolation, escalation	escalation
FREQ_058 - Predefined playbooks	
FREQ_014 - SOAR	

UC_08 – Proactive threat hunting

Figure Diagram Sequence : UC_08 – Proactive threat hunting

Use case	UC_08 – Proactive threat hunting
Goal	UC_08 addresses proactive threat hunting in historical and current data beyond regular alerts.

	The Analyst deliberately searches for suspicious behaviour patterns (TTPs, IOCs) that have not yet triggered an incident or alert, saves hunting scenarios and can directly create new incidents from the findings.

Precondition	Historical and current logs/telemetry are available
Precondition	At least a basic set of hunting queries or scenarios exists
Precondition	The Analyst has access to dashboards and tools for ad-hoc queries
Postcondition	At least one hunting run has taken place
Postcondition	The findings are documented and linked to incidents or the knowledge base
Postcondition	The hunting scenarios are saved for reuse
Basic Path	Basic Path
Step	**Activity**
1	Selection of the hunting target
2	Opening of the hunting workspace
3	Creation or selection of a query / scenario
4	Launching a hunting run over the data
5	Analysis of findings
6	Conversion of findings into incidents or enrichment of existing incidents
7	Saving of the hunting scenario
8	Documentation of results
9	Planning of repeated hunting
ALT_01 – Hunting reveals nothing significant	Alternate
Step	**Activity**
1	The hunting query returns no suspicious findings or all findings are legitimate after review; the Analyst saves the hunting record
ALT_02 – Hunting reveals an extensive campaign	Alternate
Step	**Activity**
1	Hunting identifies several related findings that indicate a more extensive attack; the Analyst creates a parent incident/campaign, assigns all related findings and incidents to it and informs the Manager of the need for increased attention.
ALT_03 – The query is too demanding or slow	Alternate
Step	**Activity**
1	The launched hunting query runs over a large volume of data and the systems evaluate it as too demanding; the system alerts the Analyst
Linked functional requirements	
	Efficient work with data –
FREQ_078 - Support for ML/AI algorithms for threat detection	Use of artificial intelligence algorithms to detect anomalies and threats. Support for ML/AI algorithms for threat detection
FREQ_024 -	

Proactive threat hunting	• CTI data • manual analysis in the case of suspicious entities • the results are documented as playbooks
FREQ_048 - Full-text and fast search	

UC_09 –

Figure Diagram Sequence : UC_09 – Manage Threat Intelligence and indicators of compromise

Use case	UC_09 –
Goal	UC_09 addresses Threat Intelligence management: receiving and integrating CTI feeds, working with indicators of compromise (IOCs), their deduplication and tracking over time. The objective is for the SOC to be able to manage threats centrally, enrich incidents and logs with TI information and keep order in observables.

Precondition	TI sources are available
Precondition	Integrations with TI sources are configured
Precondition	The system has storage for TI and IOCs
Postcondition	TI data are loaded, normalized and stored
Postcondition	Redundant or conflicting IOCs are deduplicated or merged
Postcondition	IOCs/observables are linked to incidents, cases or assets and have a traceable history
Basic Path	Basic Path
Step	**Activity**
1	Loading TI from external sources
2	Normalization and storage of TI
3	Deduplication and merging of IOCs
4	Management of the IOC life cycleManagement of the IOC life cycle
5	Linking of IOCs to incidents and cases
6	Publishing TI to other parts of the system
7	Monitoring of TI quality
ALT_01 –	Alternate
Step	**Activity**
1	When TI is being loaded, the source is temporarily unavailable or returns errors; the system records an integration incident, uses the last valid set of IOCs and alerts the Administrator to the problem.
ALT_02 – Conflicting information about the same threat	Alternate
Step	**Activity**
1	Multiple TI sources provide different or contradictory information about the same IOC; the system retains all variants with their sources, marks the IOC as conflicting and leaves it to the Analyst to select the more trustworthy source.
ALT_03 – The IOC is assessed as outdated or unreliable	Alternate
Step	**Activity**

1	The Analyst finds that the given IOC is no longer relevant or has been marked as an error; changes its status to inactive, adds a comment and the system ensures that it is no longer used in new detections.
Linked functional requirements	
FREQ_043 - Threat Intelligence (CTI) integration	Integration with threat sources (IOC, TTP), automatic data enrichment. Threat Intelligence (CTI) integration
FREQ_145 - Adding and tracking observables	
FREQ_018 - Threat Intelligence	threats, TTPs and IOCs
FREQ_108 - Deduplication of threats and information	Removal of redundant IOCs and indicators. Deduplication of threats and information
FREQ_101 - Support for tactical CTI	Working with indicators of compromise (IOC) and their recording, processing and distribution. Support for tactical CTI (IOC, IP, hash, URL, domains)

UC_10 –

Figure Diagram Sequence : UC_10 – Manage compliance, metrics and management reporting

Use case	UC_10 –
Goal	UC_10 addresses the “top floor” of SOCaaS – so that management and auditors have an overview of: how well the SOC is performing (KPIs, SLAs, incident trend), whether the system complies with standards/regulations, whether all important matters are traceable retrospectively through reports, logs and audits.

Precondition	The system collects data on incidents, responses, playbooks and TI over the long term
Precondition	Defined metrics/KPIs and SLAs exist
Precondition	At least a basic compliance policy is set (standards, internal directives)
Postcondition	The Manager and the Auditor have clear metrics and reports on the state of security and SOC services available
Postcondition	Problems identified in KPIs/SLAs or compliance are recorded and have recommendations/measures assigned
Postcondition	The reports created are archived and retrievable for future audits
Basic Path	Basic Path
Step	**Activity**
1	The Manager opens the SOC management overview
2	Selection of the area of interest
3	Display of aggregated metrics and trends
4	Identification of deviations or problems
5	Detailed drill-down
6	Submission of a request for a report / analysis
7	Recording of findings and recommendations
8	Linking to measures
	Alternate

ALT_01 – Unavailable or incomplete metrics	
Step	**Activity**
1	
ALT_02 – Identified breach of an SLA or a standard	Alternate
Step	**Activity**
1	The metrics and reports show that SLAs or the requirements of a standard have been breached; the Manager registers the finding as an official finding and launches internal measures (e.g. a service quality incident, corrective measures).
Linked functional requirements	
FREQ_098 - Policies for compliance with standards	
FREQ_020 - Reporting and retrospective analysis	
FREQ_157 - Ensuring retrospective traceability and analysis of incidents	
Use case	UC_10a –
Goal	UC_10a extends UC_10 with detailed tracking of KPIs, SLAs and the overall state of security. The Manager, Auditor or Operator view trend charts, overviews by teams/customers and the overall “health status” of SOCaaS in the dashboards.

Precondition	From UC_10 – the management overview is available.
Precondition	KPIs and SLAs are defined (e.g. MTTR, MTTD, % of incidents within the SLA).
Postcondition	Identified deviations in KPIs/SLAs are documented.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	
2	The system displays a dashboard with KPIs and SLAs (include UC_02a –
3	The Manager filters the metrics by period, team, incident type or customer.
4	The system displays trend charts, averages, SLA fulfilment percentages and comparisons with target values.
5	The Manager identifies problems (e.g. a specific team has long response times) and marks them for detailed analysis or corrective measures.
ALT_10a_01 – KPIs or SLAs are not yet defined	Alternate
Step	**Activity**
1	data sources.

Linked functional requirements	
FREQ_073 - Collection of system metrics, processes and behaviour	
FREQ_159 - Creation of a basic overview of the state of security and incidents	incidents
Use case	UC_10b – Creation and scheduling of management and compliance reports
Goal	UC_10b addresses practical work with reports for management and audits: creation, configuration of content, scheduling of regular reports and their one-off generation.

Precondition	The system has aggregated data from the other UCs (incidents, TI, playbooks, KPIs) at its disposal.
Precondition	The user has sufficient permissions to create reports.
Postcondition	Report templates for management/the regulator are created.
Postcondition	Both regular and ad-hoc reports are set up according to needs.
Basic Path	Basic Path
Step	**Activity**
1	The Manager or the Auditor opens the “Reports” section within UC_10.
2	Selects the report type (management overview, incident overview, compliance report).
3	– selection of metrics, time period, filters.
4	The user chooses whether it is a one-off report or a regular one (daily/weekly/monthly).
5	– PDF/CSV/…
6	The generated report is saved and is available in the report archive.
ALT_01 – Incomplete report due to missing data	Alternate
Step	**Activity**
1	
Linked functional requirements	
FREQ_025 - Creation of reports and dashboards	• incident overviews • visualizations from metrics and ticketing • exports for audit and SLA reporting
FREQ_162 - Scheduling of regular reports	
– time period, incident types	– time period, incident types
Use case	UC_10c –
Goal	UC_10c addresses the security and audit aspect of reporting: who sees what, who made what accessible, whether reports are archived and whether it is possible to reconstruct who had which data available.

Precondition	Generated reports exist in the system (UC_10b).
Precondition	Roles and access policies (RBAC) are defined.
Postcondition	Access to reports is restricted according to roles and responsibilities.
Postcondition	An audit trail exists of who worked with the reports and when.

Postcondition	Important reports are archived for the purposes of future audits.
Basic Path	Basic Path
Step	**Activity**
1	The Manager or the Auditor opens the management of reports and access.
2	For individual report types, sets which roles or specific users have access to them.
3	
4	
5	
ALT_01 – Attempt to access a report without authorization	Alternate
Step	**Activity**
1	
Linked functional requirements	
FREQ_066 - RBAC and audit trail	Role-based access control and logging of changes in the system. RBAC and audit trail

UC_11 –

Figure Diagram Sequence : UC_11 – Manage the customer's assets and environment

Use case	UC_11 –
Goal	The objective of UC_11 is for SOCaaS to know what it is actually protecting – all relevant customer assets (servers, applications, networks, cloud services...) and their relationships. It makes it possible to record assets, distinguish their types, map them to locations/VLANs/IPs and track their life cycle, so that incidents, threats and vulnerabilities can be linked to specific parts of the environment.

Precondition	The customer has been onboarded in the system (UC_00) and has a basic profile created.
Precondition	The system has a module / section for asset recording at its disposal.
Precondition	
Postcondition	
Postcondition	
Postcondition	Changes to assets (addition, modification, decommissioning) are recorded and the life cycle is traceable.
Basic Path	Basic Path
Step	**Activity**
1	The Operator opens the “Assets” module for a specific customer.
2	
3	
4	The Administrator adds technical data – IP addresses, hostname, environment (prod/test/dev).
5	

6	The Operator sets the life-cycle status of the asset (e.g. “in operation”, “being deployed”, “decommissioned”).
7	The system saves the asset record and makes it available to other modules (incident mgmt, TI, vuln mgmt, reporting).
8	Upon a further change (upgrade, migration, decommissioning), the Administrator updates the asset record and the system records the change in the history.
ALT_11_01 – Import of assets from an external CMDB	Alternate
Step	**Activity**
1	Instead of creating records manually, the Operator chooses an import from an external CMDB or inventory tool; the system loads the list of assets, displays a preview and allows them to be saved in bulk or matched with existing records.
ALT_11_02 – Duplicate asset detected	Alternate
Step	**Activity**
1	When a new asset is being saved, the system detects that a record with the same key identifiers (e.g. IP/hostname) already exists; us
ALT_11_03 – Change of asset criticality	Alternate
Step	**Activity**
1	
Linked functional requirements	
FREQ_017 - Asset inventory and management	
FREQ_114 - Creation, editing and deletion of asset records	assets
	Management of the individual phases of the asset life cycle — decommissioning)
FREQ_115 - Distinguishing assets by type	– hardware, software, virtual, cloud
FREQ_118 - Mapping of assets to locations, VLANs, IP ranges, racks	

UC_12 –

UC_12 covers vulnerability management in SOCaaS:
from receiving the outputs of vulnerability scanners, through their assignment to specific assets (UC_11) and prioritization according to risk, to the planning and tracking of corrective measures.
The aim is to have a comprehensive overview of where we have security gaps, what is most important to fix and within what time.

Figure Diagram Sequence : UC_12 – Manage vulnerabilities and security findings

Use case	UC_12 –
Goal	UC_12 covers vulnerability management in SOCaaS: from receiving outputs from vulnerability scanners, through their assignment to specific assets (UC_11) and prioritization according to risk, to the planning and tracking of corrective measures. The objective is to have a comprehensive overview of where we have security holes, what is most important to fix and in what time frame.

Precondition	Vulnerability scan results or other security findings exist

Precondition	Assets are recorded in the system
Precondition	A basic vulnerability prioritization policy is defined
Postcondition	Vulnerabilities are recorded and assigned to specific assets.
Postcondition	
Postcondition	The resolution status (unfixed / in progress / fixed / accepted risk) is tracked and traceable.
Basic Path	Basic Path
Step	**Activity**
1	Import or entry of vulnerabilities
2	Normalization and grouping of findings
3	Assignment of vulnerabilities to assets
4	Calculation and setting of vulnerability priorityCalculation and setting of vulnerability priority
5	Creation of a remediation plan
6	Implementation of corrective measures
7	Re-scan or status verification
8	Vulnerability status update
9	Reporting and linking with incidents
ALT_12_01 –	Alternate
Step	**Activity**
1	ger decides after discussion whether the risk is temporarily accepted or compensating measures are introduced (network segmentation, increased monitoring). The vulnerability status is set to “accepted risk” or “compensated”.
ALT_12_02 – Duplicate or obsolete finding detected	Alternate
Step	**Activity**
1	relevant; the finding is marked as duplicate or obsolete, while a reference record is retained for audit.
ALT_12_03 –	Alternate
Step	**Activity**
1	
Linked functional requirements	
FREQ_097 - Support for EPSS – prediction of vulnerability exploitation	Use of vulnerability exploitation probability models. Support for EPSS – prediction of vulnerability exploitation
FREQ_023 - Vulnerability management and inventory	• Assets are updated on the basis of detection • vulnerability-related incidents are linked to the management system
FREQ_019 - Vulnerability management	
FREQ_074 - Collection of information on vulnerabilities and configurations	Obtaining information on vulnerabilities from configuration data and comparison with CVE databases. Collection of information on vulnerabilities and configurations
FREQ_086 - Updates of vulnerability tests – community and enterprise feed	Frequency and scope of detection pattern updates. Updates of vulnerability tests – community and enterprise feed

UC_13 –

Figure Diagram Sequence : UC_13 – Design and maintain the security architecture of the customer's SOCaaS environment

Use case	UC_13 –
Goal	UC_13 addresses the design and ongoing maintenance of the technical and security architecture for a specific customer: how the customer is connected to SOCaaS, which systems, zones and logging sources are integrated, through which channels the data flow (agent, syslog, API, VPN, peering…), how SIEM, SOAR, TI, ticketing, EDR, vuln scanners and asset mgmt are interconnected. The output is an approved and maintained architectural design (topology, integration points, data flows) and a list of mandatory log sources and log types, which serves as a basis for onboarding (UC_00), monitoring (UC_01), asset management (UC_11), vulnerability management (UC_12) and automation (UC_07).

Precondition	
Precondition	The customer has provided the necessary overview of their environment (at least the high-level architecture, types of systems, networks).
Precondition	
Postcondition	There is a documented and approved architectural design for connecting the customer's environment to SOCaaS (topology, integration points, data flow).
Postcondition	Integration channels are defined (which system → in what way → into which SOCaaS module).
Postcondition	Changes to the architecture are traceable (versions, who approved them, when) and usable as input for onboarding and operation.
Postcondition	A list of mandatory log sources and log types for onboarding the customer to SOCaaS is defined and documented (including the minimum fields required for threat detection).
Basic Path	Basic Path
Step	**Activity**
1	Collection of requirements and inputs
2	Analysis of the customer's existing architecture
3	Design of data flows and integration patterns, including the identification of mandatory log sources and log types
4	Design of integrations with the customer's tools
5	Assessment of security principles and risks
6	Approval of the architectural design
7	Submission of the design for implementation
8	Ongoing maintenance of the architecture
ALT_13_01 –	Alternate
Step	**Activity**
1	design so that it uses alternative integration patterns or a narrower scope of monitoring and resubmits the changes for approval.
ALT_13_02 – Changes in the customer's environment after deployment	Alternate
Step	**Activity**
1	Over time, the customer adds new systems, migrates to

	the cloud or changes the topology; the Architect creates a revision of the architectural design, adds new integration points, and the Operator plans and carries out the necessary changes to the SOCaaS configuration.
ALT_13_03 – The design does not pass the security or performance assessment	Alternate
Step	**Activity**
1	During the assessment of the design, it is found that the proposed solution is not satisfactory (excessive latencies, unacceptable risks, insufficient scaling); the design is returned to the Architect for rework and is resubmitted for approval only after the comments have been incorporated.
Linked functional requirements	
FREQ_030 - Integration with other components	Connection to data sources Integration with incident management and SOAR tools Knowledge base and playbooks
FREQ_166 - Integration with tools such as SIEM, Ticketing, Incident recording, Asset management, CTI	incidents, Asset management, CTI, ...
FREQ_120 - Integration with monitoring, SIEM, ticketing system, EDR, vulnerability scanner, incident records	system, EDR, vulnerability scanner, incident records
FREQ_095 - Integrations with tools such as PaloAlto, Fortinet, Cisco, Nagios, Splunk, Verinice	, Verinice
FREQ_013 - Integration with other tools	

UC_14 –

Figure Diagram Sequence : UC_14 – Work with the customer portal and collaborate

Use case	UC_14 –
Goal	UC_14 addresses the customer's view of SOCaaS – via a web portal where: sees their incidents, KPIs, reports and assets, they can collaborate with the SOC (comments, attachments, approval of measures), they can customize the portal for multiple organizations/units. The portal is a modern, responsive, multi-tenant web interface and also supports more advanced settings (templates, sharing, integration hooks in sub-UCs).

Precondition	The customer has been onboarded (UC_00) and has at least one organization / tenant created.
Precondition	Accounts have been created for users and roles assigned (e.g. “Security Manager”).
Precondition	The portal is accessible via a secure web interface (HTTPS, SSO/Federation if needed).
Postcondition	Through the portal, the user has an overview of their incidents, KPIs and assets.
Postcondition	
Postcondition	The portal respects the multi-tenant model – data are separated between organizations and the settings are tailored to the needs of the specific organization.
	Basic Path

Basic Path	
Step	**Activity**
1	The end user logs in to the customer portal (SSO / username + password / MFA according to policy).
2	The system displays the home overview – a dashboard with the status of incidents, basic KPIs and notifications
3	
4	
5	
6	
7	
8	The system records all interactions (access to incidents, comments, changes to settings) for audit purposes and ensures that they are visible only within the given organization.
ALT_14_01 – The user has no organization assigned	Alternate
Step	**Activity**
1	After login, the system finds that the account is not linked to any organization; it displays information about the missing assignment and recommends
ALT_14_02 – Restricted view according to role	Alternate
Step	**Activity**
1	The user has only a role with restricted rights (e.g. “read-only”); the portal hides some action elements (editing, approval) and allows only the viewing of incidents and reports.
Linked functional requirements	
FREQ_141 - Modern, responsive web interface	Modern and responsive design for convenient use. Modern, responsive web interface
ing of tasks and observables between organizations	
Use case	UC_14a –
Goal	UC_14a extends UC_14 with specific work with incidents/tickets from the customer's perspective: view the list of incidents, open the detail, create a new “ticket” or add information, change statuses (New, In progress, Closed, Postponed), purposefully route the incident to the right resolver (L1/L2/L3, a specific team).

Precondition	The precondition from UC_14 applies – the user is logged in and has an organization.
Precondition	
Postcondition	Incidents/tickets are created or updated according to the customer's actions.
Postcondition	The incident has its current status set and a resolver assigned.
Basic Path	Basic Path
Step	**Activity**
1	In the portal, the user opens the “Incidents / Tickets”

	section.
2	The system displays a list of incidents with a filter by status, type, priority or period.
3	The user selects a specific incident and opens its detail.
4	progress”).
5	
6	The system saves the changes, updates the view in the portal and makes them available to SOC analysts.
ALT_14a_01 –	Alternate
Step	**Activity**
1	creates a new record and assigns it to the SOC queue.
ALT_14a_02 – Status change is not permitted	Alternate
Step	**Activity**
1	The system rejects the change and displays information about insufficient rights.
Linked functional requirements	
FREQ_131 - Assignment to a specific resolver	Assignment of tickets to specific resolvers, including escalation by level. Assignment to a specific resolver (L1 analyst, escalation L2/L3)
FREQ_129 - Creation and editing of records	Basic functionality of a ticketing system – creating, editing and deleting tickets. Creation and editing of records (tickets)
	Closed, Postponed)
Use case	UC_14b –
Goal	UC_14b extends UC_14 with a collaboration layer for incident handling: comments between the customer and the SOC, e-mail notifications about status changes, comments and deadlines, an audit trail of all changes and accesses in the ticket.

Precondition	The incident exists and is available in the portal (UC_14a).
Precondition	
Postcondition	Comments and/or any status changes initiated by the customer are added to the incident.
Postcondition	All changes and accesses are recorded for audit purposes; the relevant parties receive notifications.
Basic Path	Basic Path
Step	**Activity**
1	The user opens the incident detail in the portal.The user opens the incident detail in the portal.
2	The system saves the comment and records who added it and when.
3	The system saves the comment and records who added it and when.
4	The system sends email notifications to the relevant parties (Analyst, other customer representatives) about a new comment or status change.
5	The Analyst replies via their tool; the reply is synchronized to the portal and displayed to the customer as a further comment.
6	

ALT_14b_01 – Notifications are turned off for a specific user	Alternate
Linked functional requirements	
FREQ_142 - Recording of all changes, accesses and comments in the ticket	Recording of all actions, changes and comments in a ticket. Recording of all changes, accesses and comments in a ticket
FREQ_132 - E-mail notifications about status changes, comments, deadlines	Automatic e-mail notifications of status changes, comments, deadlines. E-mail notifications of status changes, comments, deadlines
Use case	UC_14c –
Goal	UC_14c extends UC_14 with the configuration part for the customer: setting incident priorities and severity from the customer's perspective, setting up integration channels (REST API / Webhooks) for connecting the portal to the customer's internal tools (ticketing, chat, ITSM).

Precondition	
Precondition	At least basic incident priorities and categories are defined for the organization.
Postcondition	Preferred incident priorities/severities are defined for the given organization.
Postcondition	Integration channels are configured (if needed) – e.g. Webhooks for notifications to internal ticketing.
Basic Path	Basic Path
Step	**Activity**
1	The Manager opens the “Organization settings” section in the portal.
2	a).
3	In the “Integrations” section, enters the endpoint URL for Webhooks or API tokens for connecting to the internal ticketing/ITSM system.
4	The system verifies basic connectivity and saves the settings.
5	On further changes to the incident status or for new incidents, the system sends notifications via REST API / Webhooks to the customer's systems according to the settings.
ALT_14c_01 – Invalid or unavailable integration interface	Alternate
Step	**Activity**
1	When the integration settings are saved, the test request fails (timeout, 4xx, 5xx); the system alerts the Manager and either saves the integration as inactive or requires the parameters to be corrected.
Linked functional requirements	
FREQ_139 - Support for REST API and Webhooks	Support for REST API interfaces and Webhooks for communication with other systems. Support for REST API and Webhooks
FREQ_135 - Setting incident priority and severity	Setting the priority and severity level of a ticket for better planning. Setting the priority and severity of an incident

UC_15 –

Figure Diagram Sequence : UC_15 – Manage the operation of the SOCaaS platform

Use case	UC_15 –
Goal	UC_15 addresses the technical operation of the SOCaaS platform so that: it is stable, performant and available, agents and sensors do not burden the customer's environment unnecessarily, the platform is continuously updated (signatures, modules), processing/scanning capacity is kept under control. The objective is for SOCaaS to run reliably, to be able to handle the expected volume of data and not to jeopardize the performance of the customer's systems.

Precondition	The SOCaaS platform is deployed in the production environment (on-prem/cloud/SaaS).
Precondition	Monitoring tools and mechanisms exist for tracking the status of the platform and the agents.
Precondition	Basic operating parameters are defined –
Postcondition	The status of the platform and the deployed agents is continuously monitored and known to the Operator.
Postcondition	Updates of signatures and modules are performed in a controlled manner and without significant service outage.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	
2	The system continuously monitors the status of agents deployed at customers –
3	When the number of customers or the data volume grows, the Operator evaluates the processing/scanning capacity and compares it with the expected growth.
4	Based on the update policy, the Operator schedules regular updates of signatures and modules (e.g. off-peak) to minimize the impact on performance.
5	The system performs the updates and verifies whether the agents and components are functional after the update and report to the expected extent.
6	
7	All operational interventions (updates, configuration changes, capacity interventions) are recorded for audit and diagnostic purposes.
ALT_15_01 –	Alternate
Step	**Activity**
1	configuration (scanning frequency, data scope), or proposes an expansion of capacity or an optimization of the deployment.
ALT_15_02 – Failure of signature or module update	Alternate
Step	**Activity**
1	Operator identifies the affected systems, rolls them back to the last stable version or repeats the update with adjusted parameters.

Linked functional requirements	
FREQ_085 - Estimated scanning capacity	
FREQ_053 - System status monitoring	Monitoring of system performance, availability and functionality. System status monitoring (healthcheck)
FREQ_082 - Simple centralized management of agents	Central console for the management, configuration and supervision of all agents. Simple central management of agents
FREQ_083 - Regular updates of signatures and modules	Regular updates of threat databases, signatures and detection rules. Regular updates of signatures and modules

UC_16 –

Figure Diagram Sequence : UC_16 – Adapt reports, exports and documents to the organization's needs

Use case	UC_16 –
Goal	UC_16 addresses the configuration of the form of SOCaaS outputs: the appearance of reports according to corporate identity (logo, colours, header), export formats (CSV, XML, PDF, HTML, Markdown), export of incidents and documents for further processing or archiving. It follows on from UC_10b (which addresses the content and scheduling of reports) by enabling detailed configuration of presentation and export, so that the outputs fit into the customer's environment and tools.

Precondition	
Precondition	
Precondition	The SOCaaS platform supports multiple export formats and basic appearance templates.
Postcondition	Report appearance templates are defined for individual organizations (logo, colours, header).
Postcondition	Preferred export formats are set for specific types of reports/incidents.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The Manager or Auditor opens the “Report and export settings” section in the portal.
2	
3	In the Appearance section, selects or modifies the template:
4	n).
5	
6	After confirmation, the system saves the appearance template and the preferred export formats for the given report/document type.
7	
8	organization.
ALT_16_01 – The required export format is not supported	Alternate
Step	**Activity**
1	. CSV instead of XLSX, PDF instead of DOCX).

ALT_16_02 – Error when exporting a large volume of data	Alternate
Step	**Activity**
1	When a report with a large number of records is being exported, a limit or timeout is exceeded; the system interrupts the export, informs the user and offers to narrow the scope (shorter period, filtered data) or an asynchronous export.
ALT_16_03 – Change of corporate identity	Alternate
Step	**Activity**
1	The organization changes its logo or corporate colours; the Manager opens the appearance settings, adjusts the template (logo, colours) and after saving, will be
Linked functional requirements	
FREQ_153 - Export of incidents to CSV, PDF formats, via REST API	Data export for documentation or reporting. Export of incidents to CSV, PDF formats, via REST API
FREQ_164 - Customization of the visual form of the report	
FREQ_180 - Export of documents to PDF, HTML or Markdown format	
FREQ_169 - Web/GUI interface for creating and managing reports	User-friendly interface for designing, editing and managing reports. Web/GUI interface for creating and managing reports
FREQ_092 - Configurable report formats	Flexibility of outputs for further processing. Configurable report formats (e.g. CSV, XML, PDF)

UC_17 –

Figure Diagram Sequence : UC_17 – Manage users and roles in the SOCaaS platform

Use case	
Goal	UC_17 addresses the administration of users and roles within SOCaaS: creation and modification of accounts, assignment of roles (SOC, customer, auditor…), setting up access via RBAC, adding custom attributes where applicable. It is a system/administrator UC that supports all other UCs by determining who can see and do what in the platform.

Precondition	The SOCaaS platform is running and has an accessible administrative web interface.
Precondition	The currently logged-in user has administrator permissions to manage accounts and roles.
Postcondition	Created, modified or deactivated user accounts are stored in the system.
Postcondition	Users are assigned appropriate roles according to the RBAC model.
Postcondition	Any custom attributes/metadata are set and usable in other parts of the system.
	Basic Path

Basic Path	
Step	**Activity**
1	The Operator logs in to the administrator web interface.
2	They open the “Users and roles” section.
3	
4	When creating an account, enters basic data (name, contacts, account identifier) and selects one or more user roles (e.g. SOC analyst, Manager, Customer, Auditor).
5	
6	The system saves the changes and displays the user in a clear list; the interface allows filtering and searching by name, role and other attributes.
7	
ALT_17_01 – Attempt to make a change for which the user does not have permission	Alternate
Step	**Activity**
1	sufficient permission.
ALT_17_02 – Invalid combination of roles	Alternate
Step	**Activity**
1	When the account is being saved, the system detects that the selected combination of roles is in conflict with the RBAC policy (e.g. conflict of interest); the administrator
Linked functional requirements	
	etBox/Django)
FREQ_180 - Export of documents to PDF, HTML or Markdown format	
FREQ_164 - Customization of the visual form of the report	
FREQ_092 - Configurable report formats	Flexibility of outputs for further processing. Configurable report formats (e.g. CSV, XML, PDF)
FREQ_178 - RBAC support	Access control based on user roles. RBAC support – different levels of access for reading, editing, approval
FREQ_153 - Export of incidents to CSV, PDF formats, via REST API	Data export for documentation or reporting. Export of incidents to CSV, PDF formats, via REST API
FREQ_181 - Simple and intuitive interface for editing and publishing records	User-friendly GUI for knowledge management. Simple and intuitive interface for editing and publishing entries
FREQ_169 - Web/GUI interface for creating and managing reports	User-friendly interface for designing, editing and managing reports. Web/GUI interface for creating and managing reports
FREQ_150 - Support for multiple user roles	RBAC support for different roles. Support for multiple user roles – at least analyst and administrator

UC_18 –

Figure Diagram Sequence : UC_18 – Manage organizations, teams and case structure

Use case	UC_18 –
Goal	UC_18 addresses the administration of organizations/tenants and the way incidents/cases are structured within them: creating and modifying organizations / teams, setting up categories, types and owners of cases,

	defining incident templates and the way they are shared between teams and external partners. It builds on UC_17 (users and roles) and UC_14 (customer portal) and supplements them with an “organizational-process” layer.

Precondition	The user is logged in and has permissions to manage organizations/case structure.
Precondition	SOCaaS has at least a few users created (UC_17) and at least one organization/tenant (UC_14).
Postcondition	Organizations/teams have a case structure set up (types, categories, owners).
Postcondition	Templates for recurring incidents and the way they are shared between teams/partners are defined.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The Manager or Operator opens the “Organizations and cases” section in the administration.
2	They select an existing organization (tenant) or create a new one and assign teams to it (e.g. “SOC L1”, “SOC L2”, “Customer IT”).
3	For the organization, they set the case/incident types (e.g. “Phishing”, “Malware”, “Policy”, “Vuln finding”) and basic categories.
4	For individual incident types, creates templates – pre-filled fields, recommended items, required information.
5	Assigns owners, tags and categories (e.g. “critical”, “regulatory”, “internal”) to incident types and templates so that it is possible to
6	
7	The system saves the organization structure, templates and sharing rules; new incidents are created according to these settings.
ALT_18_01 – Creating a custom case type for a specific organization	Alternate
Step	**Activity**
1	The organization has a specific case type (e.g. “Compliance finding”) that does not exist in the global schema; the Manager adds a new case type for this organization only and creates a custom template for it.
ALT_18_02 – Restriction of case sharing with an external partner	Alternate
Step	**Activity**
1	and adjusts the sharing rules so that these cases are accessible only to internal teams.
Linked functional requirements	
FREQ_147 - Categorization of incidents using tags	
FREQ_158 - Sharing cases between teams and external partners according to rights	Support for controlled sharing of cases. Sharing cases between teams and external partners according to rights
	e, under maintenance, decommissioned)

UC_19 –

Figure Diagram Sequence : UC_19 – Manage the retention, protection and auditing of SOCaaS data

Use case	UC_19 –
Goal	UC_19 addresses data management in SOCaaS from the platform perspective: where and how logs are stored, indexed and retained, which retention policies apply to individual log sources, how logs are protected and encrypted, how audit records of the activities of users and analysts are kept. The objective is for SOCaaS to meet the requirements for secure storage and auditability of data, and at the same time to support forensic analysis.

Precondition	The SOCaaS platform is in operation (UC_15) and receives logs from various sources (UC_01).
Precondition	There is a log/data storage (SIEM / data lake) that supports the configuration of retention and encryption.
Precondition	At least a basic log retention and security policy is defined (e.g. according to log type or regulation).
Postcondition	Retention policies are set for logs/data according to source and importance.
Postcondition	Logs are protected both in transit and at rest (encryption configured).
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	Design of the storage and retention architecture
2	Setting retention policies according to source and importance
3	Enabling and verifying log encryption
4	Configuring the collection of audit records
5	Monitoring the status of retention and the audit trail
6	Evaluating auditors' requirements
7	Adjusting policies based on findings
ALT_19_01 – Insufficient capacity for the configured retention	Alternate
Step	**Activity**
1	With longer retention periods, the Operator finds that the storage does not have sufficient capacity; together with the Architect, they either adjust the retention (e.g. differently according to log type) or propose an expansion of the storage.
ALT_19_02 – Auditor's requirement for longer retention	Alternate
Step	**Activity**
1	The Auditor or regulator requires a longer retention period for a specific type of logs (e.g. login logs); the Architect and the Operator adjust
ALT_19_03 – Incident involving compromise of the	Alternate

log storage	
Step	**Activity**
1	Operator, based on the findings, tighten the encryption, access rights or storage segmentation.
Linked functional requirements	
FREQ_039 - Supported log formats	CEF, LEEF...)
FREQ_051 - Retention	
FREQ_071 - Collection of audit data using agents	Collection of audit records of user activities, processes and the system via an agent. Collection of audit data using agents
FREQ_052 - Encryption	Protection of logs against unauthorized access in transit and at rest. Encryption (both in transit and at rest)
FREQ_154 - Logging of analysts' activities during incident handling (audit trail)	Recording of activities for forensic analysis. Logging of analysts' activities during incident handling (audit trail)

UC_20 –

Figure Diagram Sequence : UC_20 – Manage the knowledge base and playbook library

Use case	UC_20 –
Goal	UC_20 ensures that the SOC has, in a centralized and managed manner: the knowledge base (KB) – articles, guides, lessons learned, procedures, the playbook library – both manual and automated response procedures, the process of approving, versioning and publishing this content.

Precondition	There is a module for the knowledge base and playbooks available to the Analyst and the Manager.
Precondition	Roles and rights for creating, editing and approving content are defined.
Precondition	At least basic KB articles or playbooks (e.g. an initialization set) already exist in the system.
Postcondition	The knowledge base contains up-to-date, versioned and categorized records.
Postcondition	The playbook library contains published and usable playbooks linked to incident types.
Postcondition	Each entry has a traceable history and information on who created and approved it.
Basic Path	Basic Path
Step	**Activity**
1	
2	The Analyst creates a new entry or opens an existing one and adds content based on current knowledge from incidents, TI or hunting.
3	The Analyst assigns the entry to incident types, categories and tags so that it can easily be found in other UCs.
4	The Analyst saves the record as a draft and submits it for approval to the Manager or the area owner.
5	The Manager reviews the content, compares the changes with the previous version and decides whether to approve it or return it for revision.
6	After approval, the system marks the new version as valid and moves the old version to the history with a record of

	the date and the author of the change.
7	The valid entry is made available in the relevant parts of the system (e.g. in the incident detail, in the playbook engine, in the customer portal).
8	The system records all operations on the record (creation, edits, approval) for audit and forensic analysis.
ALT_20_01 – The record is returned for further work	Alternate
Step	**Activity**
1	The Manager does not approve the proposed content, adds a comment with remarks and the record is returned to the Analyst in the draft state.
ALT_20_02 – The entry is marked as obsolete	Alternate
Step	**Activity**
1	but it remains available in the history.
Linked functional requirements	
	EM
FREQ_140 - Export to PDF, CSV, JSON formats for documentation and reporting	
FREQ_174 - Support for structured documents – categories, sections, labels	Organization of KB documents according to structured rules (categories, tags, sections). Support for structured documents – categories, sections, labels (tags)
FREQ_175 - Full-text search with support for filters and tags	
FREQ_173 - Creation, editing and versioning of records	playbooks, FAQ)
Use case	UC_20a –
Goal	UC_20a addresses in detail the life cycle of KB articles – creation, editing, structure, tagging and linking to incidents.

Precondition	The preconditions of UC_20 apply.
Precondition	
Postcondition	The KB contains up-to-date, structured articles with rich content, change history and an audit trail.
Basic Path	Basic Path
Step	**Activity**
1	The Analyst opens the list of KB articles in the “Knowledge Base” module.
2	The Analyst creates a new KB article or opens an existing entry for editing.
3	The Analyst edits the content of the article and adds structure (sections, subsections), tags and categories.
4	The Analyst inserts relevant attachments, logs or screenshots that help in resolving similar incidents.
5	The Analyst saves the entry; the system records the author and time of the change and, if necessary, submits it for approval.
ALT_20a_01 - Merging two related KB entries	Alternate
Step	**Activity**
1	The Analyst identifies two very similar articles in the knowledge base, creates one consolidated entry and marks the original articles as archived with a reference to the new consolidated article.
	Alternate

ALT_20a_02 - Attempt to edit without sufficient permissions	
Step	**Activity**
1	permissions and leaves the entry unchanged.
Linked functional requirements	
FREQ_183 - Records of who edited the document and when	Audit trail of document changes with information on authors and time. Records of who edited a document and when
Use case	UC_20b –
Goal	UC_20b addresses the design, editing and maintenance of playbooks that the SOC uses for automated or semi-automated response (UC_07).

Precondition	A workflow/playbook engine is available in the system.
Precondition	
Postcondition	Playbooks have defined steps, branching and integration points and are tested before deployment to production.
Basic Path	Basic Path
Step	**Activity**
1	The Analyst or Developer opens the “Playbooks” section in the SOCaaS interface.
2	The user creates a new playbook or opens an existing one for editing.
3	In the graphical editor, they define the individual steps of the playbook, their order, branching and execution conditions.
4	
5	The user runs a test of the playbook in debug/simulation mode and verifies that the steps proceed as expected.
6	After a successful test, they submit the playbook to the Manager for approval and, once approved, it is marked as “production” for UC_07.
ALT_20b_01 - The playbook fails the test in simulation mode	Alternate
Step	**Activity**
1	After the playbook test is run in simulation mode, the system detects an error in one of the steps or missing parameters; the test ends with an error and the playbook remains in the draft state until the Analyst or Developer modifies it.
ALT_20b_02 - Saving a playbook with an incomplete configuration	Alternate
Step	**Activity**
1	rejects the saving and highlights the missing or invalid settings.
Linked functional requirements	
FREQ_067 - Playbook debugging & testing	
	without the need for programming
FREQ_060 - Workflow engine with branching, conditions and loops	
Use case	UC_20c –
Goal	UC_20c addresses the governance layer over the KB and

	playbooks – approval, versioning, change audit and the approval workflow.

Precondition	Drafts or modified versions of KB articles and playbooks exist (UC_20a, UC_20b).
Precondition	
Postcondition	Each entry has a status (draft, under approval, published, archived) and a tracked history of changes and authors.
Basic Path	Basic Path
Step	**Activity**
1	The Manager opens the list of KB articles and playbooks awaiting approval.
2	The Manager selects a specific entry and displays the current version together with an overview of changes compared with the previous version.
3	The Manager decides whether to approve the entry, return it for rework or mark it for archiving.
4	Upon approval, the system sets the new version as valid, moves the older version to the history and records the date and author of the approval.
5	According to the configured workflow, the system informs the relevant users that the new article or playbook has been published and is available for use.
ALT_20c_01 - Error in content detected after publication	Alternate
Step	**Activity**
1	After a new version of a KB article or playbook has been published, the Analyst notices a factual error, creates a corrective version and submits it for expedited approval; once approved, the corrective version becomes valid.
ALT_20c_02 - The primary approver is not available	Alternate
Step	**Activity**
1	The entry is awaiting approval, but the primary Manager is unavailable for a long period; after a defined time has elapsed, the system offers the approval to a substitute approver according to the configured approval workflow.
Linked functional requirements	

UC_21 –

Figure Diagram Sequence : UC_21 – Manage and evaluate machine learning models for incident detection

Use case	UC_21 –
Goal	UC_21 addresses the life cycle of the ML models that we use to detect incidents and anomalies in SOCaaS: design and training of models, quality measurement (FP/FN, accuracy, speed), robustness against changes in data,

	adaptive/online learning while the system is running.

Precondition	SOCaaS has ML-based detection component(s) (anomalies, classifiers, scoring).
Precondition	Historical data/logs are available for training and testing the models.
Precondition	
Postcondition	
Postcondition	
Postcondition	The model evaluation results are recorded for further decision-making and audit.
Basic Path	Basic Path
Step	**Activity**
1	The Data Scientist selects a dataset (historical logs, incidents) as the basis for training or testing the model.
2	The Data Scientist trains a new model or modifies an existing model based on current detection requirements.
3	The system evaluates the quality of the model on the validation set, including the metrics of false alarms and missed incidents (FP/FN).
4	
5	– the time required to process new events under conditions close to real operation.
6	and the detection quality
7	If the model meets the required metrics, the Manager approves its deployment to production and the Operator ensures the deployment of the model in the detection engine.
8	After deployment, the system continuously collects feedback from real operation (actual FP/FN) and prepares materials for further tuning or adaptive learning.
ALT_21_02 – The model is too slow for real time	Alternate
Step	**Activity**
1	architecture, simplifies the model or proposes offloading to another environment (e.g. a dedicated GPU server).
ALT_21_03 – Significant data drift appears after deployment	Alternate
Step	**Activity**
1	Over time, it is found that new types of events or behaviour have reduced the detection quality; the system warns of drift, the Data Scientist prepares an updated training set and launches adaptive/online learning so that the model reflects the new data.
ALT_21_01 – The model has too high a number of false alarms (FP)	Alternate
Step	**Activity**
1	After evaluation, it turns out that the model generates an unacceptably high number of FPs; the Data Scientist adjusts the architecture, hyperparameters or threshold values and repeats the training and evaluation process until an acceptable level is achieved.
Linked functional requirements	

FREQ_193 - Adaptive/online learning	
FREQ_186 - False alarm rate	t FP/FN.

UC_22 –

Figure Diagram Sequence : UC_22 – Manage and deploy detection packages and rules

Use case	UC_22 –
Goal	UC_22 addresses the life cycle of detection content (rules, correlation rules, signatures, “content packs”) in SOCaaS: the design and modification of detection rules and packages, testing on historical or synthetic data, controlled deployment to production, including the possibility of rollback, restricted deployment for selected tenants/customers. UC_22 does not address the detection runtime itself (that is in UC_03), but the process of designing, testing and the controlled deployment of detection rules and packages to the engine.

Precondition	There is a detection engine (UC_03) that supports the configuration of rules/packages.
Precondition	The platform has a mechanism for testing rules (a separate test environment or test mode).
Precondition	
Postcondition	New or modified detection rules are tested, approved and deployed to production, or rejected.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The Analyst opens the “Detection rules and packages” module and displays the list of existing rules.
2	The Analyst creates a new rule or modifies an existing one, defining conditions, threshold values and the mapping to an incident type.
3	The Analyst saves the change as a proposal (draft) and runs a test of the rule on historical or synthetic data in test mode.
4	The system evaluates the test results – the number of hits, potential false alarms and the impact on existing detection.
5	Based on the test results, the Analyst modifies the rule if necessary and repeats the test until acceptable behaviour is achieved.
6	The Analyst submits the rule for approval to the Manager or to the defined owner of the detection content.
7	The Manager assesses the impact of the rule (in particular on the number of alerts, threat types and affected customers/tenants) and decides whether to approve it or return it for modification.
8	After approval, the Developer / DevSecOps launches the deployment of the rule to production, or only for selected tenants or in restricted (“canary”) mode.
9	The system records all changes (rule version, author, approver, deployment time) and monitors the impact on alerts and performance.

ALT_22_01 – The rule test reveals an extremely high number of hits	Alternate
Step	**Activity**
1	After step 4, the Analyst finds that the rule would generate a disproportionate number of alerts; modifies the rule (tightening conditions, adding filters) and repeats the test until an acceptable number of hits is achieved.
ALT_22_02 – The deployed rule negatively affects production	Alternate
Step	**Activity**
1	After deployment in step 8, the system detects a significant increase in the number of alerts, latency or errors; the Operator or DevSecOps initiates a rollback to the previous version of the rules and the new rule is marked as “requires modification/test”.
ALT_22_03 –	Alternate
Step	**Activity**
1	During approval in step 7, the Manager decides that the rule is relevant only for a certain type of customer (e.g. a specific sector or tenant); during deployment, only a subset of tenants to which the rule is applied is selected
Linked functional requirements	
FREQ_042 - Machine Learning/Behavioural analysis	
FREQ_044 - Anomaly detection	Detection of non-standard behaviour or deviations from expected behaviour. Anomaly detection
FREQ_040 - Real time vs. batch processing	
FREQ_022 - Incident detection and escalation	known threats. After detection: • an alert is generated • the alert is automatically transformed into an incident • Zammad provides ticketing for the L1 team and escalation support, • the team evaluates the observables and uses enrichment
FREQ_075 - Log analysis and correlation with threats	Log analysis aimed at detecting correlated events and potential threats. Log analysis and correlation with threats

UC_23 –

Figure Diagram Sequence : UC_23 – Manage and operate vulnerability scanning

Use case	UC_23 –
Goal	UC_23 addresses the operation and management of vulnerability scanning within SOCaaS: planning and launching scans, assigning scans to assets and networks, the technical architecture of scanning (master/sensor),

	integration of findings into tickets and into the vulnerability management process (UC_12).

Precondition	At least the basic assets and network ranges (UC_11) intended for scanning are known.
Precondition	A vulnerability scanning tool (on-prem, VM or SaaS) is deployed in the environment.
Precondition	
Postcondition	Vulnerability scanning for the selected ranges has taken place according to the schedule or on demand.
Postcondition	Findings are enriched with CPE/CVE and CVSS scores and are available for UC_12.
Postcondition	Relevant findings are exported or linked to remediation tickets.
Basic Path	Basic Path
Step	**Activity**
1	The Operator or Administrator opens the “Vulnerability scanning” module and displays an overview of existing scanning profiles.
2	The Operator selects the ranges (IPs, networks, asset groups) and chooses the scan type (full, quick, authenticated).
3	
4	
5	After the scan is completed, the system processes the results, assigns CPE/CVE identifiers to the vulnerabilities and calculates the CVSS score.After the scan is completed, the system processes the results, assigns CPE/CVE identifiers to the vulnerabilities and calculates the CVSS score.
6	addressed.The Analyst or Administrator displays the scan results, filters the findings by severity and scope and marks those that
7	The system creates or updates remediation tickets in the integrated ticketing system or exports the findings in the selected format for further processing.
ALT_23_01 –	Alternate
Step	**Activity**
1	During the scan, some systems are unavailable or are blocked by a firewall; the system marks these parts as “not scanned”, the Oper
ALT_23_02 –	Alternate
Step	**Activity**
1	
Linked functional requirements	
FREQ_096 - Support for CVSS 4.0	Support for the latest version of the CVSS scoring system. Support for CVSS 4.0
FREQ_087 - Support for CPE, CVE identifiers	
FREQ_090 - Support for scheduling tasks and alerts	
FREQ_091 - Remediation tickets – integration or export	– integration or export
FREQ_094 - Scanning architecture	

UC_24 – Orchestration of integrations between SOCaaS and external systems

Figure Diagram Sequence : UC_24 – Orchestration of integrations between SOCaaS and external systems

Use case	UC_24 – Orchestration of integrations between SOCaaS and external systems
Goal	UC_24 addresses the technical and process orchestration of integrations between SOCaaS and other systems: SIEM, SOAR, CTI, ticketing, communication tools, firewall, EDR, API integrations, webhooks, plug-ins and connectors, unified management of data flows and actions across these systems. The objective is for incident response, automation (UC_07) and incident management to function as one interconnected ecosystem, not as isolated tools.

Precondition	The integration architecture of the customer and SOCaaS has been designed (UC_13) and at least a basic connection to SIEM/SOAR/ticketing exists.
Precondition	The SOCaaS platform supports REST API, webhooks and a plug-in/connector mechanism.
Precondition	
Postcondition	The defined integration links and flows between SOCaaS, SIEM, SOAR, CTI, ticketing, firewalls, EDR and other systems are active and monitored.
Postcondition	Incidents and events are consistently synchronized between systems (status, ID, links).
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The Operator opens the “Integrations and orchestration” module and displays an overview of existing integration links (SIEM, SOAR, CTI, ticketing, EDR, firewall, communication tools).
2	The Developer or Operator creates a new integration link or modifies an existing one, selects the target system (e.g. ticketing system, CTI, firewall) and the integration type (API, webhook, plug-in).
3	The user configures authentication, endpoints, data formats and field mapping between SOCaaS and the target system.
4	→ create ticket, incident status change → update ticket, IOC from TI → update the block list in the firewall).
5	
6	customers/tenants.
7	–
8	The system continuously logs successful and unsuccessful integration calls, displays statistics and alerts the Operator to errors or outages of integration channels.
ALT_24_01 – Integration call failure	Alternate
Step	**Activity**
1	During a test or production API/webhook call, the external system returns an error or is unavailable; SOCaaS marks the record as unsuccessful, stores the error details and, depending on the settings, either repeats the call using a retry policy or creates an internal incident/report for the Operator.
	Alternate

ALT_24_02 – Conflict in data mapping between systems	
Step	**Activity**
1	When setting up the field mapping between SOCaaS and the external system, it is found that some mandatory fields in the target system are not moe which the integration is used.
Linked functional requirements	
FREQ_063 - API-first approach	
FREQ_138 - Integration with SIEM, SOAR, CTI, incident tracking tools,reporting and asset management tools	Integration with other security tools for automation and workflow. Integration with SIEM, SOAR, CTI, incident recording tools,reporting and asset management tools
FREQ_064 - Support for plug-ins and connectors	
FREQ_152 - Connection to SIEM, SOAR, ticketing and reporting systems and other systems via API or plugins	
FREQ_062 - Orchestration between systems: SIEM, CTI, ticketing, communication tools, firewall, EDR	Interconnection and data exchange with other systems within the incident response process. Orchestration between systems: SIEM, CTI, ticketing, communication tools, firewall, EDR

UC_25 –

Figure Diagram Sequence : UC_25 – Manage threat intelligence (CTI) and the IOC lifecycle

Use case	UC_25 –
Goal	UC_25 addresses the complete CTI lifecycle in SOCaaS: obtaining CTI from various sources (feeds, MISP, open-source, vendor), normalization, enrichment and prioritization of CTI data, distribution of IOCs/TTPs to detection (SIEM, EDR, firewall, SOAR) and to incidents.

Precondition	SOCaaS has a CTI module (or is integrated with an external CTI tool).
Precondition	CTI sources (community, commercial, internal) are defined, together with a basic policy on which sources are “trusted”.
Precondition	Detection systems (SIEM, EDR, firewall, IDS, SOAR) support the reception of IOCs/TTPs from CTI.
Postcondition	CTI data are systematically collected, normalized, enriched and aggregated.
Postcondition	Threats are prioritized and inputs for detection, hunting and incidents are created from the relevant IOCs/TTPs.
Postcondition	IOCs/TTPs are distributed to the detection systems and incident management in a consistent manner (with an audit trail).
Basic Path	Basic Path
Step	**Activity**
1	The Analyst opens the “Threat Intelligence” module and displays an overview of active CTI sources and the latest updates.
2	Periodically or on demand, the system downloads new CTI data from all configured sources (open-source, community, vendor, internal).Periodically or on demand, the system downloads new CTI data from all configured sources (open-source, community, vendor, internal).

3	The CTI pipeline normalizes, enriches and aggregates the data – merges IOCs, adds context, links them with historical incidents and logs.
4	specific customers).
5	and incidents.
6	For selected IOCs/TTPs, the CTI module creates outputs for detection (e.g. block lists, SIEM rules, hunting queries) and prepares them for distribution to the connected systems.
7	In incidents and hunting tools, the Analyst has enriched CTI available – they can see campaigns, TTPs, groups and related IOCs.
8	The system continuously records which CTI sources and IOCs/TTPs were used in real incidents and hunting cases and uses this information for further fine-tuning of scoring and relevance.
ALT_25_01 –	Alternate
Step	**Activity**
1	Over time, it turns out that a specific CTI source has poor-quality or duplicate data, or is unavailable for a long period; the Manager or CTI specialist deactivates the source or reduces its weight in the scoring.
ALT_25_02 – CTI surplus and analyst overload	Alternate
Step	**Activity**
1	The system detects that the number of new IOCs/threats significantly exceeds the analysts' capacity; the CTI specialist adjusts the scoring, filters and thresholds so that only the most relevant threats come to the fore (e.g. by sector, geolocation, asset exposure).
ALT_25_03 – CTI mismatch between customers/tenants	Alternate
Step	**Activity**
1	A given IOC is relevant only to a specific customer (e.g. according to its technologies or geography); the system supports per-tenant filtering of CTI, so IOCs/TTPs are distributed only to the customers they concern.
Linked functional requirements	
FREQ_112 - Support for the largest number of authoritative CTI sources	A broad selection of community, public and paid sources. Support for the largest number of authoritative CTI sources
FREQ_100 - Support for operational CTI	(TTPs, group profiling)
FREQ_113 - Reducing the need for manual analysis	Automation and prioritization of threats so that analysts deal only with relevant ones. Reducing the need for manual analysis – saving analysts' time
FREQ_168 - Support for various sources: databases, logs, API outputs	
FREQ_099 - Support for strategic CTI	Obtaining and analysing information on long-term trends, impacts of attacks and strategic recommendations. Support for strategic CTI (reports, impact analyses, attack trends)
Use case	UC_25a –
Goal	UC_25a addresses the ingest and connection of CTI sources: defining sources (feeds, MISP, API, vendor portals), automated downloading,

	use of standardized formats.

Precondition	The CTI module is available in SOCaaS.
Precondition	The CTI sources to which we have access are known (API keys, URLs, authentication).
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The Developer opens the “CTI sources” section and displays the list of existing sources.
2	The Developer adds a new CTI source (feed, MISP, vendor API) and enters the necessary credentials.
3	
4	The system tests the connection, downloads a data sample and verifies the format and consistency.
5	After a successful test, the source is marked as active and included in regular CTI ingestion.
ALT_25a_01 – Error when connecting to a CTI source	Alternate
Step	**Activity**
1	The test in step 4 fails (invalid API key, expired token, unavailable endpoint); the system displays an error, deactivates the source and leaves it in the state “requires configuration fix”.
ALT_25a_02 – Limit or quotas on the CTI source	Alternate
Step	**Activity**
1	SOC analyst
Linked functional requirements	
FREQ_103 - Support for Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo	Ready-made connectors or integrations for well-known CTI sources. Support for Abuse.ch, Malware Bazaar, MISP, AlientVault OTX, Anomali Limo
FREQ_102 - Automated collection from open-source, community and internal sources	ce, community and internal sources
FREQ_111 - Support for formats such as STIX/TAXII	Use of standardized formats for the exchange of CTI data. Support for formats such as STIX/TAXII
Use case	UC_25b –
Goal	UC_25b addresses the CTI processing pipeline: normalization of various formats into a unified model, enrichment of IOCs and artefacts from external services, workflow for automatic/semi-automatic processing of CTI.

Precondition	CTI data have been downloaded from the sources (UC_25a).
Precondition	Integration services for enrichment (VirusTotal, Shodan, …) are configured.
Postcondition	CTI data are in a unified format, enriched and vetted, ready for scoring and distribution.
Basic Path	Basic Path
Step	**Activity**

1	The system receives new CTI data from the sources and stores them in a buffer for processing.
2	The CTI pipeline transforms various formats into a unified structured model (IOCs, TTPs, campaigns, meta).
3	For each IOC or relevant artefact, the pipeline optionally performs enrichment via external services (VirusTotal, Shodan, DomainTools, …).
4	The workflow engine applies the defined processing steps – deduplication, filtering, first-seen/last-seen logic and technical validations.
5	The resulting CTI records are stored in a unified form and marked with a status (new, processed, unconfirmed, discarded).
ALT_25b_01 – External enrichment is temporarily unavailable	Alternate
Step	**Activity**
1	In step 3, an external service (e.g. VirusTotal) does not respond in time; the system marks the enrichment status as “pending” and schedules a retry later without blocking the entire pipeline.
ALT_25b_02 – Conflict during normalization of CTI data	Alternate
Step	**Activity**
1	Different sources provide conflicting information for the same IOC; the pipeline flags the record for manual review by a CTI specialist, who selects or combines the correct values.
Linked functional requirements	
FREQ_107 - Semi-automated or fully automated processing and unification of data	data unification
FREQ_104 - Integration with 3rd party services	omainTools, URLScan.io
Use case	UC_25c –
Goal	UC_25c addresses the push of CTI to the rest of the ecosystem: forwarding IOCs to SIEM/IDS/EDR/firewalls, use of CTI in detection, playbooks and incidents,

Precondition	CTI data are processed and prioritized (UC_25, UC_25b).
Precondition	Integration links to the detection systems exist (UC_24).
Postcondition	The relevant IOCs/TTPs are deployed in the detection systems.
Postcondition	Incidents and hunting cases are enriched with CTI metadata.
Basic Path	Basic Path
Step	**Activity**
1	The CTI module selects the IOCs/TTPs that are marked as “relevant for distribution” according to scoring and policy.
2	
3	The system generates output artefacts (block lists, SIEM rules, feeds) and sends them via integration channels (API, plug-in, CTI interface).
4	

5	When an incident arises, SOCaaS automatically enriches the incident with information from CTI – it links IOCs, TTPs and MITRE ATT&CK techniques.
ALT_25c_01 – The detection system does not accept some IOCs	Alternate
Step	**Activity**
1	
ALT_25c_02 – The IOC is later marked as a false positive or irrelevant	Alternate
Step	**Activity**
1	Based on feedback from incidents, it is found that some IOCs cause spam in detection; the CTI module withdraws these IOCs from distribution and adjusts the scoring/policy so that similar threats are evaluated differently in the future.
Linked functional requirements	
FREQ_110 - Mapping to MITRE ATT&CK for TTP analysis and team collaboration	Linking incidents, IOCs and TTPs with the ATT&CK framework. Mapping to MITRE ATT&CK for TTP analysis and team collaboration
FREQ_109 - Integration with SIEM and firewall for use in automated detections	Forwarding IOCs and data directly to detection systems (SIEM, IDS, firewall). Integration with SIEM and firewall for use in automated detections
FREQ_148 - Automated enrichment of incident information from internal and CTI sources	Integration for enriching IOCs and metadata from CTI or other systems. Automated enrichment of incident information from internal and CTI sources

UC_26 –

Figure Diagram Sequence : UC_26 – Configure report scheduling and export

Use case	UC_26 –
Goal	UC_26 addresses the practical management of reports in SOCaaS: setting up automatic generation and distribution of reports, customization of the content and appearance of reports, generation of one-off ad hoc reports for managers or audit.

Precondition	A reporting module (UC_10) with defined report types (incidents, SLA, KPIs…) exists in the system.
Precondition	Distribution channels are configured (at least e-mail, ideally also webhook/integration endpoints).
Postcondition	Generation schedules, recipients and export formats are set for individual report types.
Postcondition	
Postcondition	Reports contain the selected metrics, charts and visualizations in the required design.
Basic Path	Basic Path
Step	**Activity**
1	The Manager or Operator opens the “Reports and export” module and displays the available report types.
2	

3	The user configures the report generation schedule (daily, weekly, monthly) and the list of recipients or target endpoints.
4	The user adjusts the appearance of the report – organization logo, header, notes and, where applicable, the structure of sections.
5	The user selects the export format (PDF, CSV, JSON) and the delivery method (e-mail, webhook, saving to storage).
6	At the defined times, the system automatically generates the report, adds the selected charts, tables and statistics and sends it to the selected channels.
7	
ALT_26_01 – Creating a one-off ad hoc report	Alternate
Step	**Activity**
1	The Manager needs an extraordinary report outside the scheduled cycle; in the module, selects the report type, sets the filters and the time period and launches a one-off generation, whereby the system generates the report only once without changing the existing schedules.
ALT_26_02 – Unsuccessful delivery of an automatically generated report	Alternate
Step	**Activity**
1	During a regular report export, an error occurs when sending the e-mail or webhook; the system saves the report, marks the distribution as un
Linked functional requirements	
FREQ_036 - Customization of report outputs	• • Personalization of design – logos, header, colour scheme • Inclusion of explanatory notes, remarks and contextual commentary
FREQ_035 - Automated export of reports	• Periodic reports – outputs generated and distributed daily, weekly or monthly. • Distribution via e-mail or webhook – • Support for templates and custom filters –b.
FREQ_140 - Export to PDF, CSV, JSON formats for documentation and reporting	

UC_27 –

Figure Diagram Sequence : UC_27 – Manage the security status and relationships of assets

Use case	UC_27 –
Goal	UC_27 extends asset management with a “smart CMDB”: records the security status of each asset (patch level, vulnerabilities, recent changes), it displays and manages the links between assets (server–service–application),

	it uses automated discovery and API integrations, it keeps an audit of changes to assets.

Precondition	A basic asset inventory has been established (UC_11) – at least the key servers, networks and applications exist.
Precondition	Data sources for discovery are available (scans, CMDB, cloud API…).
Precondition	Users have defined roles for reading/editing assets.
Postcondition	The current security status (versions, patch level, vulnerabilities) is recorded for each asset.
Postcondition	Links between assets are defined (topology / dependencies).
Postcondition	Changes to assets are auditable (who, what, when) and available for forensic and operational analysis.
Basic Path	Basic Path
Step	**Activity**
1	The Administrator or Operator opens the “Assets” module and displays an overview of assets with their current security status.
2	nts of the environment.
3	The system launches discovery and identifies new or changed assets, comparing them with the existing inventory.
4	The Administrator reviews the newly found or changed assets, assigns them to the correct categories and adjusts the details as needed (own
5	The Administrator or Architect adds or modifies the relationships between assets (e.g. server → service → application → database) so that they reflect the actual dependencies.
6	The system automatically updates the security status of assets based on inputs from scanning, patch management or other integration sources.
7	history.
ALT_27_01 – Conflict between discovery and the existing inventory	Alternate
Step	**Activity**
1	Discovery finds an asset that already exists in the inventory but with a different designation or parameters; the system flags a conflict and the Administrator chooses whether to merge the record, overwrite it or keep it as a new asset.
ALT_27_02 – Failure of automated discovery	Alternate
Step	**Activity**
1	
Linked functional requirements	
FREQ_119 - Links between assets	– service – application)
FREQ_124 - Automated discovery of assets in the network	Automated collection and updating of asset data from the network and other systems. Automated discovery of assets in the network (e.g. SNMP, nmap, APIs from other systems)
FREQ_117 - Recording the security status of each asset	Storing information on vulnerabilities, patch level and system updates. Recording the security status of each asset (e.g. OS versions, last update)
FREQ_122 - API support for asset management and integration	

FREQ_126 - Recording of changes to assets	l)

UC_28 –

Figure Diagram Sequence : UC_28 – Deploy and maintain SOCaaS in different environments

Use case	UC_28 –
Goal	UC_28 addresses the deployment and technical operation of the SOCaaS platform in various environments: on-premise at the customer, in the cloud, hybrid, as a dedicated IaaS environment for SOCaaS, with clear rules for maintenance, updates and monitoring, including the use of an open-source/free edition as the base platform. It is a technical-operational UC that extends platform operation (e.g. the UC on SOCaaS operation) with a multi-deployment / IaaS perspective.

Precondition	The architecture of the SOCaaS solution has been designed (topology, modules, integration points).
Precondition	
Precondition	The Operator has defined processes for the monitoring, maintenance and updating of components.
Postcondition	SOCaaS is deployed in the selected environment (on-prem/cloud/hybrid/IaaS) and is monitored.
Postcondition	Rules for maintenance, updates and testing of changes in a separate environment are set.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The Architect, together with the Operator, decides whether SOCaaS will be deployed on-premise, in the cloud or in a hybrid model.
2	The Operator prepares the target environment – creates the necessary virtual machines, networks, storage and other resources in IaaS.
3	The Operator installs or deploys the SOCaaS components in the chosen form (e.g. VM, Docker containers, cloud/SaaS instance).
4	The Operator sets up centralized monitoring of module functionality (metrics collection, health-checks, status logging).
5	
6	The Operator defines rules for maintenance and updates – maintenance windows, the order of deploying changes and the rollback procedure.
7	s) to ensure performance and availability.
ALT_28_01 –→ cloud or hybrid)	Alternate
Step	**Activity**
1	Based on growth or customer requirements, it turns out that the original on-prem deployment is no longer adequate; the Architect proposes a transition to the cloud or a hybrid model, and the Operator prepares the new environment and a gradual migration of components so as

	to preserve the ava
ALT_28_02 – The update causes problems in the production environment	Alternate
Step	**Activity**
1	After the update has been deployed according to steps 5–6, it is found that a module is not working correctly; the Operator uses the prepared rollback procedure, reverts to the previous version and first fixes the update and tests it in the staging environment before another attempt.
Linked functional requirements	
FREQ_093 - Deployment options: on-premise, cloud/SaaS, VM, Docker	Flexibility of installation in various environments. Deployment options: on-premise, cloud/SaaS, VM, Docker
FREQ_027 - System maintenance and updates	• rules for component updates • a test environment for verifying changes • centralized monitoring of the functionality of all modules
FREQ_037 - Support for IaaS functionality	The solution requires the full functionality of IaaS – operation of the SOC as a service.
	nia
FREQ_069 - Deployment options: on-prem, cloud, hybrid	prem, cloud, hybrid

UC_29 –

Figure Diagram Sequence : UC_29 – Explain and analyse anomalies detected by ML models

Use case	UC_29 –
Goal	UC_29 ensures that SOCaaS can comprehensibly explain anomalies detected by machine learning models: display the context of the data flow (logs, metrics, network flows), show the time course of the signals that led to the anomaly, work with unsupervised models (without labels), and give the analyst an interpretation of "why the model flagged it".

Precondition	ML models for anomaly detection are deployed in SOCaaS (UC_21) and generate anomalous events/alerts.
Precondition	– validated, normalized, enriched and stored.
Precondition	The user (Analyst, Data Scientist) has access to the "ML anomalies and explanations" module.
Postcondition	For the selected anomaly, there is an explanation of the detection – over time, over the relevant inputs and with a text comment.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	The Analyst opens the "ML anomalies" module and selects a specific anomaly or incident that was detected by an ML model.
2	The system loads all related events from the data pipeline

	— which have passed validation, normalization and enrichment and have been assigned to the correct indices and timestamps.
3	The system identifies which ML model detected the anomaly (supervised/unsupervised) and loads its outputs (score or, where applicable, cluster membership).
4	– the key signals, time segments and features that contributed most to the model's decision.
5	The system displays the time course of selected metrics and log events (time series), highlighting the interval in which the anomaly was detected.
6	The system displays the breakdown of inputs by type (logs, metrics, flow data) and shows which groups of inputs most influenced the detection, including the case when they come from different sources.
7	The Analyst adds their own interpretation, marks the detection as “true positive”, “false positive” or “unclear” and saves the feedback
ALT_29_01 – Insufficient data to explain the anomaly	Alternate
Step	**Activity**
1	When attempting an explanation, the system finds that some logs or metrics are missing in the selected time segment (the data were not stored or processed); the system warns the analyst of the limited explanation, displays only the available data and marks the explanation as “incomplete”.
ALT_29_02 – The Analyst re-evaluates trust in a specific model	Alternate
Step	**Activity**
1	The Analyst repeatedly marks the anomalies detected by one model as “false positive”; the system aggregates this feedback and displays to the Data Scientist a recommendation to review the model (or replace it with another type, including a change of threshold or architecture).
Linked functional requirements	
FREQ_192 - Flexibility of input data	–
FREQ_194 - Model explainability	analyst a comprehensible explanation of why the anomaly was detected.
FREQ_028 - Processing of data flows	• Receipt of logs and events from multiple heterogeneous sources • Validation, normalization and enrichment of data • Assignment of timestamps, identifiers and event categories • Redirection of data to suitable indices for efficient analysis • Filtering out redundant or irrelevant data • Implementation of pipeline rules and processing modules
FREQ_187 - Support for learning without labels	all models require labelled data. Unsupervised models are advantageous especially with large amounts of unlabelled data.

UC_30 –

Figure Diagram Sequence : UC_30 – Manage endpoint detection and response (EDR) within SOCaaS

Use case	UC_30 –
Goal	UC_30 addresses how SOCaaS centrally manages the EDR/XDR layer: it receives alerts and logs from EDR/antivirus/OS tools, it normalizes and enriches them, it displays the status of incidents on dashboards, it feeds them into the overall incident detection (UC_03) and response (UC_07) process.

Precondition	An EDR/AV/host-based sensor (or integration agent) is deployed on the customer's endpoints.
Precondition	SOCaaS has integration connectors for collecting logs and alerts from EDR and other security tools.
Precondition	Basic correlation rules and heuristics for detecting endpoint incidents are defined.
Postcondition	Alerts and logs from endpoint tools are received, normalized and enriched and used in incident detection.
Postcondition	The status of endpoint incidents is clearly displayed on dashboards for analysts and management.
Postcondition	Endpoint incidents are connected to automated responses (UC_07) if permitted by policy.
Basic Path	Basic Path
Step	**Activity**
1	
2	The system receives alerts and data from various security tools (EDR, AV, OS logs) and routes them into a unified processing pipeline.
3	The pipeline transforms various logs from endpoints into a unified format, adds WHOIS/GEOIP and other context and stores them in appropriate indices for correlation.
4	The detection engine (UC_03) uses normalized endpoint data in correlation rules and heuristics to identify potential incidents.
5	When an incident originating at an endpoint arises, the system displays it on the dashboards together with its context (host, user, threat type, timeline).
6	The Analyst works with the endpoint incident directly in SOCaaS – filters, sorts, drills down into the details of logs and enrichment, and, where applicable, manually escalates or closes it.
7	If a playbook is defined for the given incident type, SOCaaS invokes UC_07 and offers automated or semi-automated responses (isolation, quarantine, blocking).
ALT_30_01 – Incomplete or faulty EDR integration	Alternate
Step	**Activity**
1	The EDR tool does not send all expected types of alerts or logs; the system alerts the Operator that from the given source arriv
ALT_30_02 – Surplus of endpoint alerts (alert fatigue)	Alternate
Step	**Activity**
1	After the EDR is connected, an extremely large number of low-severity alerts arrives; the Analyst and the

	Operator adjust the filters, correlation rules and thresholds so that only relevant incidents are displayed on the dashboards and the rest remain as low-priority events in the background.
Linked functional requirements	
FREQ_054 - Receiving alerts and data from various security systems	security systems
FREQ_049 - Dashboards and their categorization	Data visualization using charts, filters and widgets. Dashboards (including interactive ones) and their categorization
FREQ_047 - Normalization and enrichment of data	Transformation of various logs into a unified format and their enrichment (e.g. WHOIS, GEOIP). Data normalization and enrichment
FREQ_065 - Dashboards for incident status and statistics	Clear display of the system status and ongoing incidents. Dashboards for incident status and statistics
FREQ_002 - Incident detection process	– is responsible for identifying anomalies, attack patterns and other threats through correlation rules and heuristic mechanisms.
Use case	UC_30a –
Goal	UC_30a addresses the deployment and life cycle of the EDR agent / sensor: installation on various OSs, updates and configuration, where applicable, use of agentless mode where an agent is not possible

Precondition	The EDR/endpoint tool that will be used in SOCaaS has been selected.
Precondition	Lists of endpoints and their OSs are available.
Postcondition	The EDR agent is deployed or configured (including in agentless mode) on the relevant endpoints.
Postcondition	Agent configurations and updates are managed centrally without code changes.
Basic Path	Basic Path
Step	**Activity**
1	
2	The Operator prepares installation packages or policies for deploying the EDR agent on supported OSs.
3	The Administrator deploys the agent (or configures an agentless connection) on selected endpoints according to the customer's policy.
4	The Operator centrally sets the configuration of the agents –
5	ení.
	Alternate
Step	**Activity**
1	ess mode (e.g. log collection via syslog, WMI, API) and marks these devices in the system as “agentless”.
Linked functional requirements	
FREQ_070 - Support for various OSs	Support for the installation and running of the agent on various operating systems. Support for various OSs (Windows, Linux, macOS)
FREQ_155 - Simple management of configurations and updates	
FREQ_089 - Without the need for agents	
Use case	UC_30b –

Goal	UC_30b addresses the actual detection of malware, intrusions and suspicious behaviour on endpoints: FIM (File Integrity Monitoring), malware detection, heuristic/behavioural analysis.

Precondition	An EDR/agent is running on the endpoints (UC_30a).
Precondition	
Postcondition	Suspicious behaviour (malware, intrusions, FIM events) is detected and mapped to incidents in SOCaaS.
Basic Path	Basic Path
Step	**Activity**
1	The EDR agent monitors changes to files, processes and system calls on the endpoint.
2	
3	The EDR engine analyses the behaviour of processes and memory to identify signs of malware or security breaches.
4	Heuristic and behavioural rules (or models) evaluate the combination of events and determine whether it is suspicious activity.
5	When thresholds are exceeded or a matching pattern occurs, the EDR creates an alert, which is subsequently processed in UC_30/UC_03 as an incident or an incident candidate.
ALT_30b_01 - Suspicious behaviour without a clear verdict	Alternate
Step	**Activity**
1	The heuristic evaluates the activity as suspicious but not strong enough for automatic classification; the EDR sends a “low confidence” a
Linked functional requirements	
FREQ_076 - Detection of malware and intrusions	Identification of malicious software and security breach incidents. Detection of malware and breaches
FREQ_077 - Heuristic and behavioural analysis	Basing detection on behaviour and heuristics rather than on signatures alone. Heuristic and behavioural analysis
FREQ_072 - File Integrity Monitoring	Real-time detection of file changes for the purposes of forensic analysis and integrity. File Integrity Monitoring (FIM)
Use case	UC_30c –
Goal	UC_30c addresses automated/semi-automated responses to endpoint incidents and their mapping to MITRE ATT&CK: device isolation, file quarantine, process blocking, linking with SOAR playbooks, secure transfer of forensic data and reports.

Precondition	Response playbooks are defined for endpoint incident types (UC_07).
Precondition	The EDR tool supports automatic actions on endpoints (isolation, quarantine, blocking).
Precondition	SOCaaS has a mapping of activities to MITRE ATT&CK.
Postcondition	Endpoint incidents are mapped to ATT&CK TTPs and

	used in reports and CTI.
Postcondition	Automated responses are performed securely and auditably, including the secure transfer of reports and forensic data.
Basic Path	Basic Path
Step	**Activity**
1	The Analyst or the system identifies an endpoint incident for which an automated response is appropriate (e.g. malware on a workstation).
2	SOCaaS assigns the relevant MITRE ATT&CK techniques to the incident and displays them in the incident detail.
3	The Analyst launches a playbook, or the system automatically evaluates the conditions and performs the action (device isolation, file quarantine, process blocking).
4	
5	The system generates a summary report on the course of the incident and the responses performed and securely sends it via an encrypted channel (e.g. to the manager or the customer).
ALT_30c_01 - The automated response is blocked by policy	Alternate
Step	**Activity**
1	The Manager has set a policy that fully automatic isolation is not permitted on critical servers; for such an incident, SOCaaS offers only a “semi-automatic” action requiring explicit confirmation by an analyst.
Linked functional requirements	
FREQ_172 - Encrypted transfers of reports during automatic distribution	Secure transfer of sensitive data via encrypted channels. Encrypted transfers of reports in automatic distribution
FREQ_079 - Mapping to the MITRE ATT&CK framework	Classification of detected activities and techniques into the MITRE ATT&CK framework for the purposes of TTP analyses. Mapping to the MITRE ATT&CK framework
FREQ_080 - Automatic responses	Automatic response to incidents, such as endpoint isolation or file quarantine. Automatic responses (e.g. device isolation, file quarantine)

UC_31 –

Figure Diagram Sequence : UC_31 – Provide a workspace for manual threat analysis (CTI workspace)

Use case	UC_31 –
Goal	UC_31 ensures that SOCaaS provides a dedicated workspace for manual threat analysis (CTI): the analyst can open a specific threat, IOC or campaign, they see normalized data from multiple CTI sources, has tools for manual examination, filtering and adding comments.

Precondition	The CTI pipeline is functional (UC_25) – CTI data have been downloaded and technically processed.
Precondition	

Postcondition	For selected threats / IOCs, there are manually added analyses and comments from the analyst.
Postcondition	
Basic Path	Basic Path
Step	**Activity**
1	
2	The system loads all available information on the given threat from the CTI storage – IOCs, descriptions, source feeds – and displays it in a unified, normalized format.
3	The Analyst uses the available tools (filtering, pivoting on IOCs, linking to incidents and logs) to manually examine the data and the context of the threat.
4	The Analyst adds their own comments, relevance assessment, recommendations and, where applicable, flags the threat for specific customers/segments.
5	reports.
ALT_31_01 – CTI data for the threat are incomplete or inconsistent	Alternate
Step	**Activity**
1	In step 2, the Analyst finds that the information on the threat from different sources is contradictory or incomplete; marks the entry as “requires completion”, adds manual notes and the CTI specialist later adjusts the sources or scoring.
ALT_31_02 – The Analyst opens the CTI workspace directly from an incident	Alternate
Step	**Activity**
1	When investigating an incident in UC_06, clicks on the linked threat/IOC; the system opens the CTI workspace already pre-filtered to the relevant IO
Linked functional requirements	
FREQ_005 - Threat management process	– enables systematic work with threat information.
FREQ_055 - Normalization and parsing of data	Transformation of input data into a standardized format for further processing. Data normalization and parsing

UC_32 –

Figure 34 : UC_32 – Monitor vulnerability scanning and synchronize the status of related incidents

Use case	UC_32 –
Goal	UC_32 addresses the operational view of vulnerability scanning and related incidents: it provides a web interface for managing scans and results (on top of the functions from UC_23), it displays which findings have already been converted into incidents, and ensures synchronization of the incident status between SIEM and SOAR so that analysts have a consistent status everywhere.

Precondition	Vulnerability scanning is technically set up and runs according to UC_23.

Precondition	There is an integration connection between SIEM and SOAR (according to UC_24).
Precondition	
Postcondition	Users have a clear web interface available through which they can see scans, their status and results.
Postcondition	Scan findings that are handled as incidents have their status synchronized between SIEM and SOAR (e.g. “open / in progress / resolved”).
Basic Path	Basic Path
Step	**Activity**
1	The Analyst or Administrator opens the “Scanning and incidents” module in the SOCaaS web interface and sees an overview of launched and scheduled scans.
2	The user selects a specific scan and displays its detail – scope, launch time, status, number of vulnerabilities found and basic statistics.
3	In the same interface, the user displays the list of scan findings, with each finding linked to its current status (new, in progress, closed) and to information on whether an incident already exists for it in SIEM/SOAR.
4	The system displays for which findings an incident has been created in SOAR and automatically verifies the status of this incident in SIEM (e.g. “open”, “assigned”, “resolved”).
5	When the status of an incident changes in SOAR (e.g. after a playbook has been executed), the UC_32 module also updates the incident status in SIEM via the integration layer so that analysts and management have consistent information everywhere.
6	
ALT_32_01 – An incident exists in SOAR, but SIEM does not know its status	Alternate
Step	**Activity**
1	In step 4, the system finds that an incident exists in SOAR for a specific finding, but there is no corresponding record in SIEM (e.g. an integration error or a historical incident); the system marks the finding as “inconsistent” and alerts the Operator to check the integration rules or manually align the incidents.
ALT_32_02 –	Alternate
Step	**Activity**
1	When loading the overview in step 1 or 2, an API error occurs (e.g. the scanner is unavailable); the UI displays a warning indicating which scans/resul
Linked functional requirements	
FREQ_068 - SOAR-SIEM synchronization of incident status	
FREQ_088 - Acceptable web interface for managing scanning and results	