imperum

Imperum User Documentation

UnderstandIng the Layout

Version

0.3.0

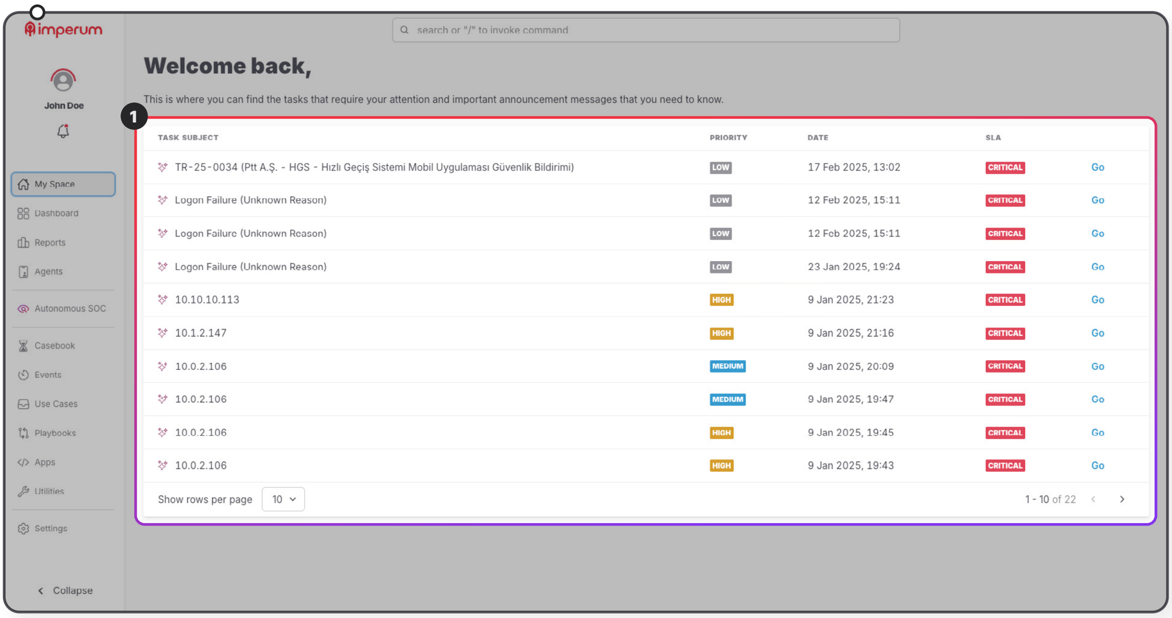
Date of Publication

November 2025

✦ Interface

Welcome to the Imperum, your comprehensive guide to understanding and utilizing the full range of capabilities offered by the Imperum platform. Imperum is designed to optimize event management, enhance security operations, and provide intelligent automation tools for efficient task management. Whether you are a security analyst, administrator, or operational team member, this documentation will guide you through the key features, workflows, and tools that Imperum offers to streamline your processes and improve productivity. This documentation serves as a comprehensive guide to understanding and utilizing the core functionalities of Imperum.

When you first open Imperum, the interface displayed will resemble the one shown above.[1] However, the content of the main screen will dynamically adjust based on the section you select from the Main Menu on the left-hand side.



Welcome back,

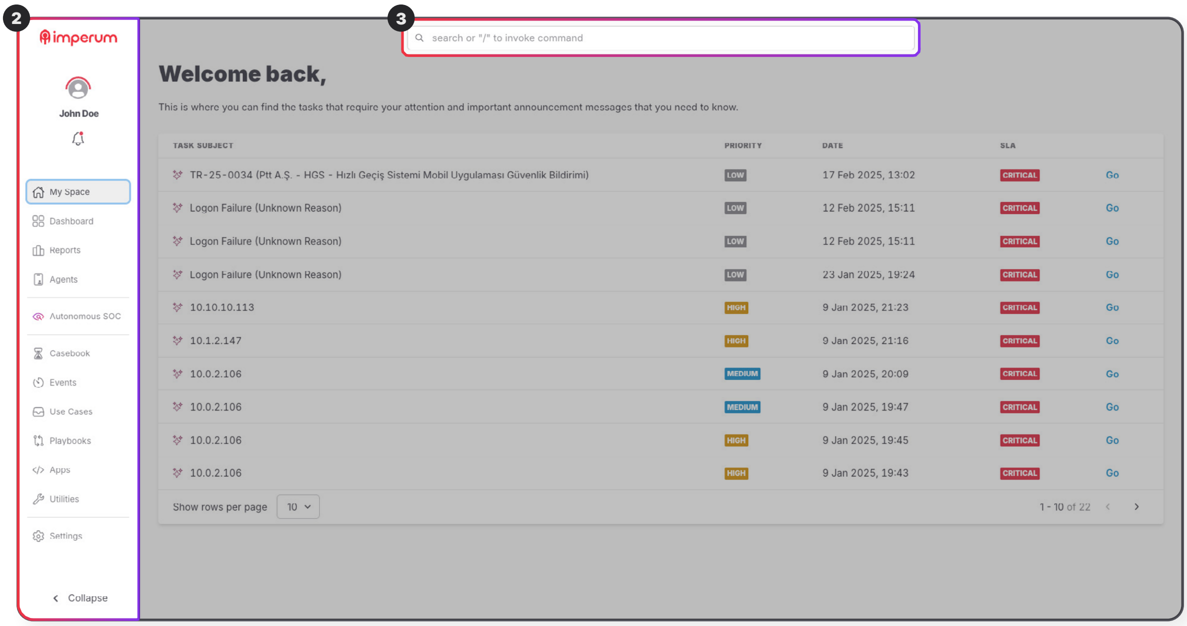
This is where you can find the tasks that require your attention and important announcement messages that you need to know.

TASK SUBJECT	PRIORITY	DATE	SLA	
TR-25-0034 (Ptt A.Ş. - HGS - Hızlı Geçiş Sistemi Mobil Uygulaması Güvenlik Bildirimi)	LOW	17 Feb 2025, 13:02	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	12 Feb 2025, 15:11	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	12 Feb 2025, 15:11	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	23 Jan 2025, 19:24	CRITICAL	Go
10.10.10.113	HIGH	9 Jan 2025, 21:23	CRITICAL	Go
10.1.2.147	HIGH	9 Jan 2025, 21:16	CRITICAL	Go
10.0.2.106	MEDIUM	9 Jan 2025, 20:09	CRITICAL	Go
10.0.2.106	MEDIUM	9 Jan 2025, 19:47	CRITICAL	Go
10.0.2.106	HIGH	9 Jan 2025, 19:45	CRITICAL	Go
10.0.2.106	HIGH	9 Jan 2025, 19:43	CRITICAL	Go

Show rows per page 10 ⌄ 1 - 10 of 22 ‹ ›

✦ Understanding the Layout: Main Menu / Search Tool:

These two elements are fixed components of the interface that remain unchanged, regardless of the section selected from the Main Menu.



Welcome back,

This is where you can find the tasks that require your attention and important announcement messages that you need to know.

TASK SUBJECT	PRIORITY	DATE	SLA	
TR-25-0034 (Ptt A.Ş. - HGS - Hızlı Geçiş Sistemi Mobil Uygulaması Güvenlik Bildirimi)	LOW	17 Feb 2025, 13:02	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	12 Feb 2025, 15:11	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	12 Feb 2025, 15:11	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	23 Jan 2025, 19:24	CRITICAL	Go
10.10.10.113	HIGH	9 Jan 2025, 21:23	CRITICAL	Go
10.1.2.147	HIGH	9 Jan 2025, 21:16	CRITICAL	Go
10.0.2.106	MEDIUM	9 Jan 2025, 20:09	CRITICAL	Go
10.0.2.106	MEDIUM	9 Jan 2025, 19:47	CRITICAL	Go
10.0.2.106	HIGH	9 Jan 2025, 19:45	CRITICAL	Go
10.0.2.106	HIGH	9 Jan 2025, 19:43	CRITICAL	Go

Show rows per page 10 ⌄ 1 - 10 of 22 ‹ ›

✦ Main Menu (Left-Side Navigation Panel):[2]

The left-hand menu acts as the core navigation hub, providing quick access to all key functionalities within the platform. Each section in the menu corresponds to a specific module or feature.

It includes the following options:

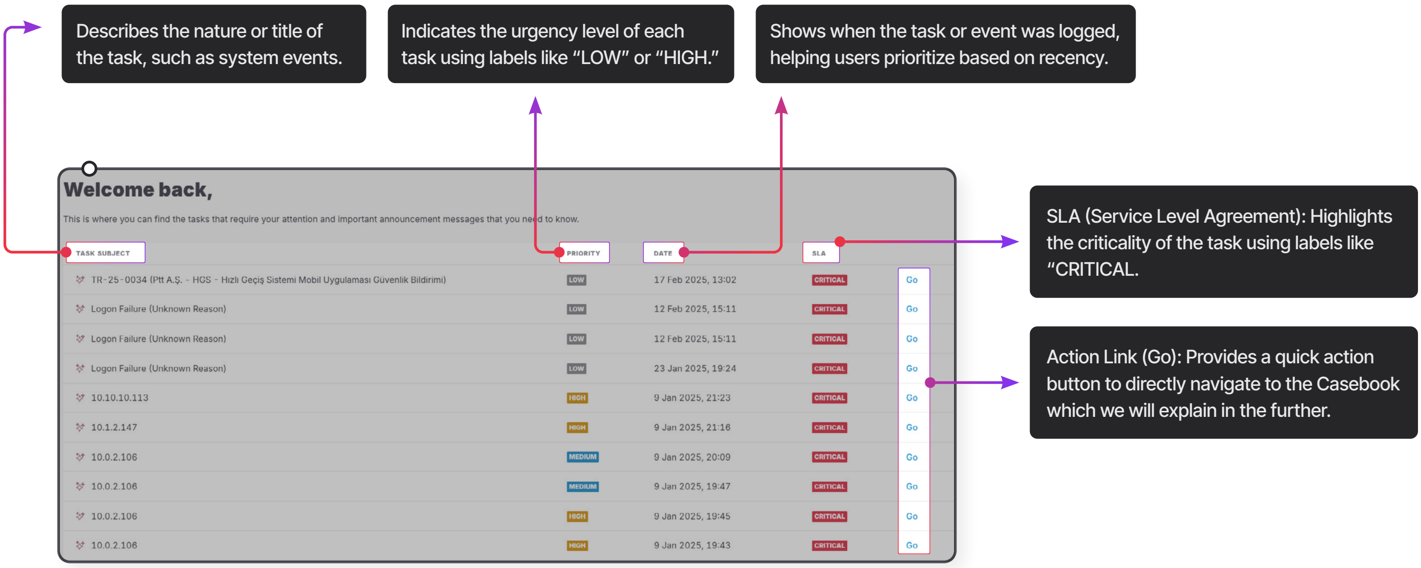
- **My Space** A personalized workspace for the user to manage tasks and settings.
- **Dashboard** An overview section displaying key metrics and real-time updates.
- **Reports** Tools for generating and accessing detailed analytical reports.
- **Agents** A section for managing system agents or automation bots.
- **Casebook** A repository for tracking cases or incidents.
- **Events** A centralized log of system events.
- **Use Cases** A library of predefined workflows or playbooks tailored for specific scenarios.
- **Playbooks** A feature for creating, managing, and executing automated workflows.
- **Apps** Integration options for third-party applications.
- **Utilities** Additional tools to support system functionality.
- **Settings** Configuration options for customizing the platform to organizational needs.

✦ Search Tool:[3]

At the top of the interface, a search bar allow users to easily locate specific items or refine the displayed data. This functionality enhances efficiency when working with large datasets or multiple workflows.

✦ My space

This is where you can find the tasks that require your attention and important announcement messages that you need to know.



Describes the nature or title of the task, such as system events.

Indicates the urgency level of each task using labels like "LOW" or "HIGH."

Shows when the task or event was logged, helping users prioritize based on recency.

SLA (Service Level Agreement): Highlights the criticality of the task using labels like "CRITICAL.

Action Link (Go): Provides a quick action button to directly navigate to the Casebook which we will explain in the further.

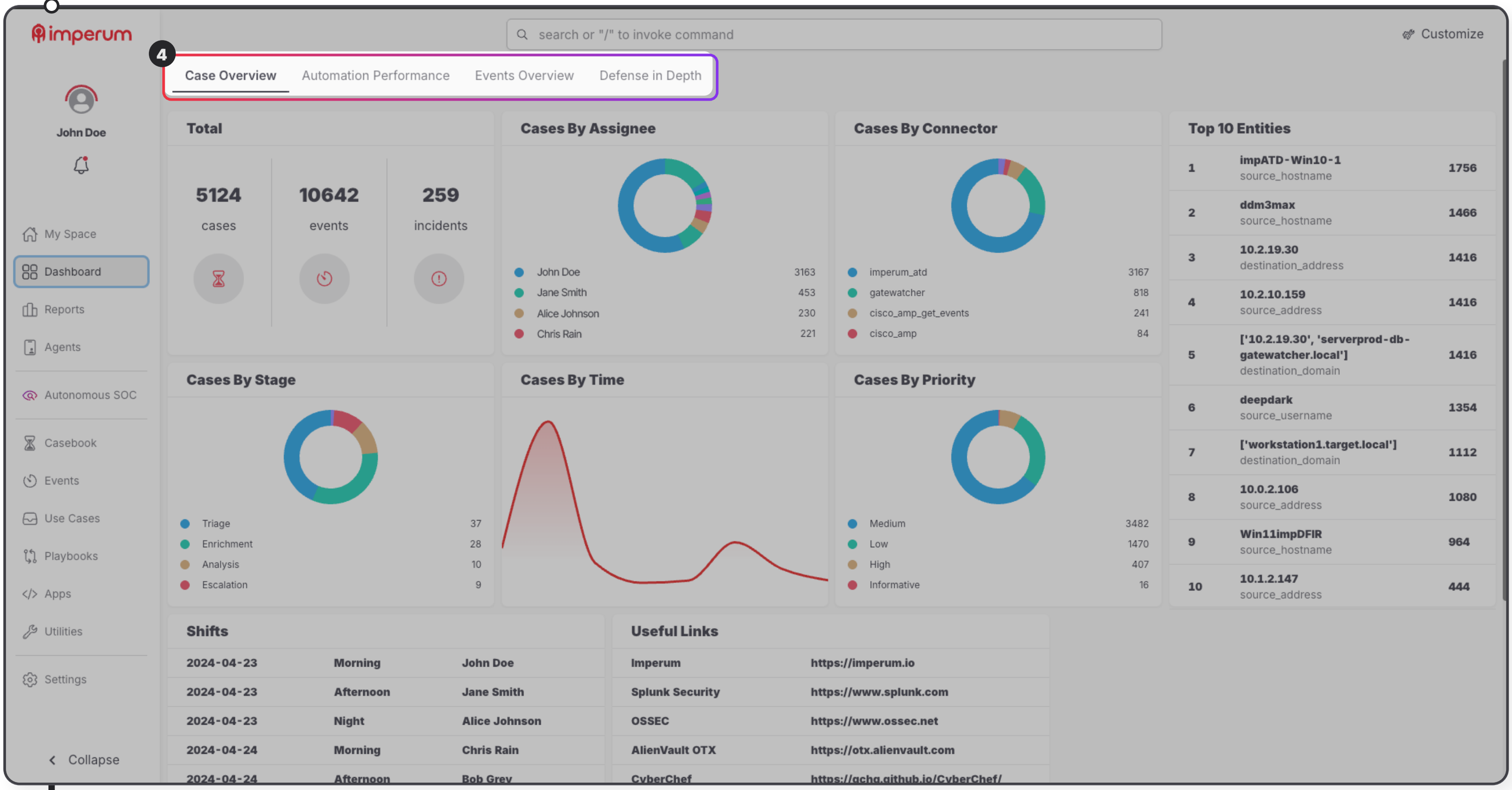
Welcome back,

This is where you can find the tasks that require your attention and important announcement messages that you need to know.

TASK SUBJECT	PRIORITY	DATE	SLA	
TR-25-0034 (Ptt A.Ş. - HGS - Hızlı Geçiş Sistemi Mobil Uygulaması Güvenlik Bildirimi)	LOW	17 Feb 2025, 13:02	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	12 Feb 2025, 15:11	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	12 Feb 2025, 15:11	CRITICAL	Go
Logon Failure (Unknown Reason)	LOW	23 Jan 2025, 19:24	CRITICAL	Go
10.10.10.113	HIGH	9 Jan 2025, 21:23	CRITICAL	Go
10.1.2.147	HIGH	9 Jan 2025, 21:16	CRITICAL	Go
10.0.2.106	MEDIUM	9 Jan 2025, 20:09	CRITICAL	Go
10.0.2.106	MEDIUM	9 Jan 2025, 19:47	CRITICAL	Go
10.0.2.106	HIGH	9 Jan 2025, 19:45	CRITICAL	Go
10.0.2.106	HIGH	9 Jan 2025, 19:43	CRITICAL	Go

✦ Dashboard

The Dashboard provides an overview of task assignments and data flow. It allows users to see how many tasks have been assigned to each individual and monitor the number and type of data pulled from the connector for each recipient. This feature offers clear insights into task distribution and data synchronization.



Total

5124	10642	259
cases	events	incidents

Cases By Assignee

●	John Doe	3163
●	Jane Smith	453
●	Alice Johnson	230
●	Chris Rain	221

Cases By Connector

●	imperum_atd	3167
●	gatewatcher	818
●	cisco_amp_get_events	241
●	cisco_amp	84

Top 10 Entities

1	impATD-Win10-1 source_hostname	1756
2	ddm3max source_hostname	1466
3	10.2.19.30 destination_address	1416
4	10.2.10.159 source_address	1416
5	['10.2.19.30', 'serverprod-db-gatewatcher.local'] destination_domain	1416
6	deepdark source_username	1354
7	['workstation1.target.local'] destination_domain	1112
8	10.0.2.106 source_address	1080
9	Win11impDFIR source_hostname	964
10	10.1.2.147 source_address	444

Cases By Stage

●	Triage	37
●	Enrichment	28
●	Analysis	10
●	Escalation	9

Cases By Priority

●	Medium	3482
●	Low	1470
●	High	407
●	Informative	16

Shifts

2024-04-23	Morning	John Doe
2024-04-23	Afternoon	Jane Smith
2024-04-23	Night	Alice Johnson
2024-04-24	Morning	Chris Rain
2024-04-24	Afternoon	Bob Grey

Useful Links

Imperum	https://imperum.io
Splunk Security	https://www.splunk.com
OSSEC	https://www.ossec.net
AlienVault OTX	https://otx.alienvault.com
CyberChef	https://gchq.github.io/CyberChef/

Header Navigation[4]

At the top, there is a navigation bar with tabs such as Case Overview, Automation Performance, Events Overview, and Defense in Depth. These allow users to switch between different analytical views.

Case Overview

This interface is part of the Case Overview dashboard, providing a high-level summary and analytical insights into the cases, events, and incidents managed within the system.

Automation Performance

Automation Performance offers a clear view of playbook performance and execution, enabling teams to monitor, analyze, and improve automated workflows.

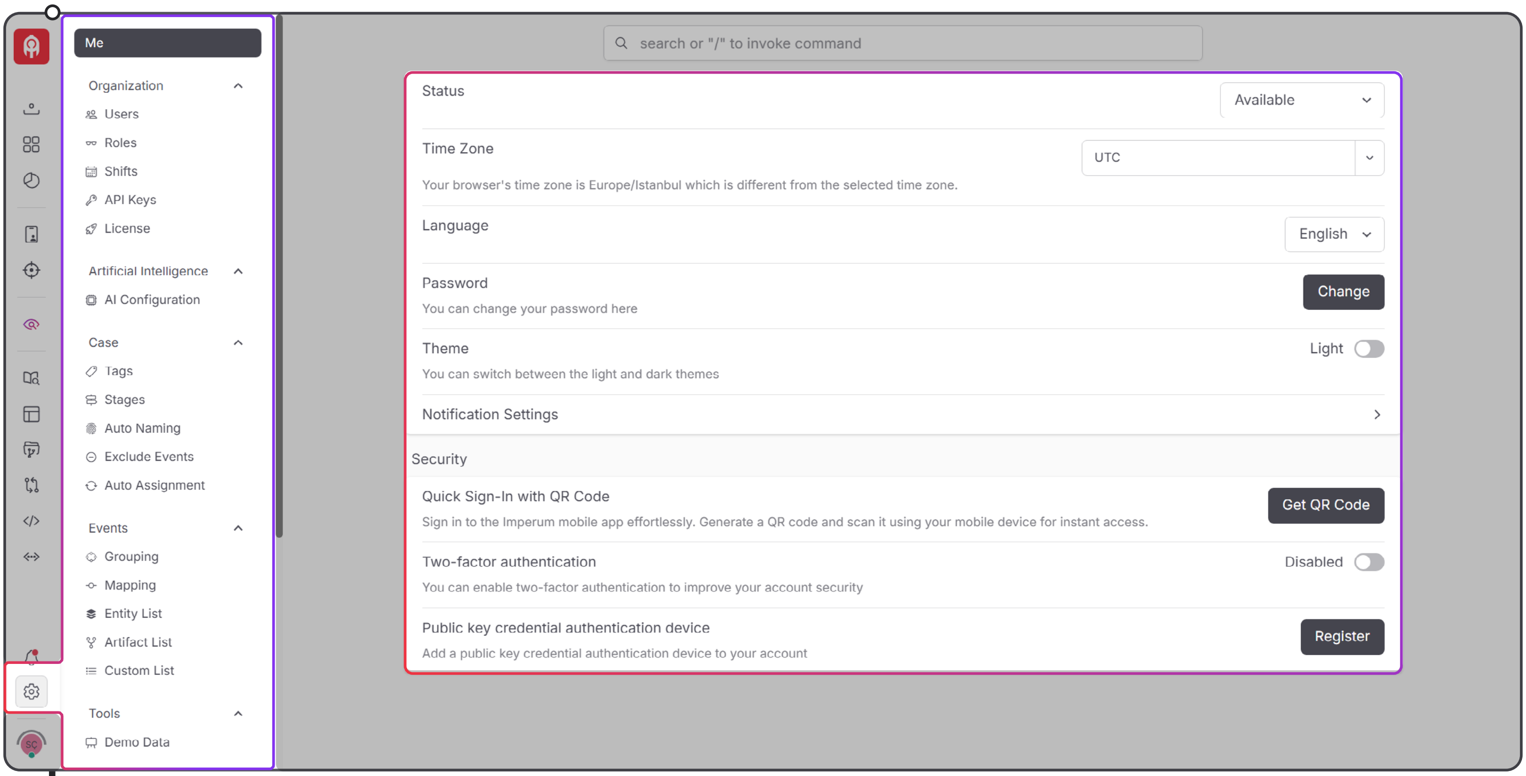
Events Overview

The Events Overview dashboard summarizes and analyzes security events, helping cybersecurity teams categorize data, detect patterns, and gain insights for incident response and threat management.

Defense in Depth

The 'Defense in Depth' dashboard analyzes an organization's layered security posture, highlighting attack trends, compromise rates, and vulnerabilities to help cybersecurity teams assess defenses and improve security measures.

✦ Settings



Status: Available

Time Zone: UTC

Your browser's time zone is Europe/Istanbul which is different from the selected time zone.

Language: English

Password — Change

You can change your password here

Theme — Light

You can switch between the light and dark themes

Notification Settings

Security

Quick Sign-In with QR Code — Get QR Code

Sign in to the Imperum mobile app effortlessly. Generate a QR code and scan it using your mobile device for instant access.

Two-factor authentication — Disabled

You can enable two-factor authentication to improve your account security

Public key credential authentication device — Register

Add a public key credential authentication device to your account

Users

Add or remove users (admin privileges required).

API Keys

Generate keys to execute actions or connectors.

Mapping

Stores app-specific mappings in an organized view.

Exclude Events

Filter out events you don't want to include, ensuring only relevant ones are processed.

Auto Assignment

Uses AI to assign cases based on previous handling, balancing workload efficiently.

Auto Naming

Automatically assigns case names. Priority: event name → source_hostname → source_address → destination_address → data_source. If none are available, a default name (New Default Case) is assigned.

Roles

View and manage user permissions.

Tags

Add or remove tags for better organization.

Custom List

Create tailored lists (e.g., duty rosters, schedules, or task organization).

Entity List & Artifact List:

Entities = people/key players; Artifacts = tools/resources they use. Together, they form the actionable components.

Configuration

Under DFIR Configuration and API Configuration, upload files to enable local agent access, streamlining communication and setup.

Grouping

Consolidates events with the same address into one case. You can set how many events are needed to trigger case creation.