imperum

# AI-Driven Autonomous SecOps

A hyperautomated platform unifying Ingestion, Detection and Response, powered by Forensic Analysis & Investigation

imperum.io

# Content

# DevOps and SecOps Challenges


The cybersecurity talent shortage, combined the increasing complexity of various GUIs and the lack of effective orchestration, is likely overwhelming your SecOps team leading to burnout and missed critical alerts.

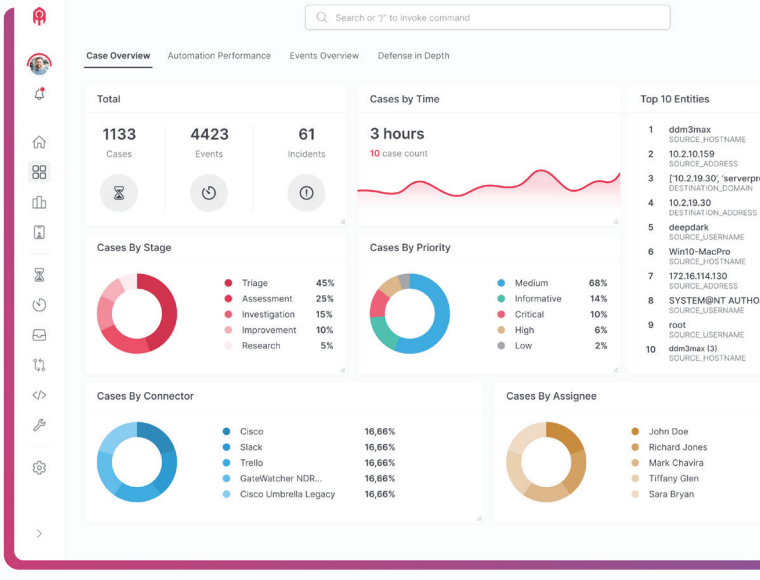
Multiple interfaces, complex front ends, and disconnected technologies are adding to your challenges, increasing complexity, inflating costs and driving up operational expenses.

# What makes Imperum the key to resolving these challenges?

We've built a solution that cuts through complexity, streamlining everything from fragmented GUIs to the lack of orchestration.

With AI-powered virtual analysts and responders, we bridge the expertise gap, reduce burnout, and ensure no critical alert is ever missed.

Take full control with our unified dashboard, powered by machine learning to identify and prioritize threats while seamlessly integrating with your existing security tools to maximize the value of your current investments.



## Autonomous SecOps Platform

# Hyperautomated Autonomous Investigation with Human-in-the-Loop

Security teams are drowning in alerts, false positives, and manual investigations. Imperum changes the game with Hyperautomated Autonomous Investigation, powered by Local AI, ensuring seamless efficiency with human expertise when needed.

**Alert Fatigue Reduction**

**70% reduction**

in manual workload by filtering false positives & correlating alerts autonomously

**Analyst Efficiency Improvement**

**70% increase**

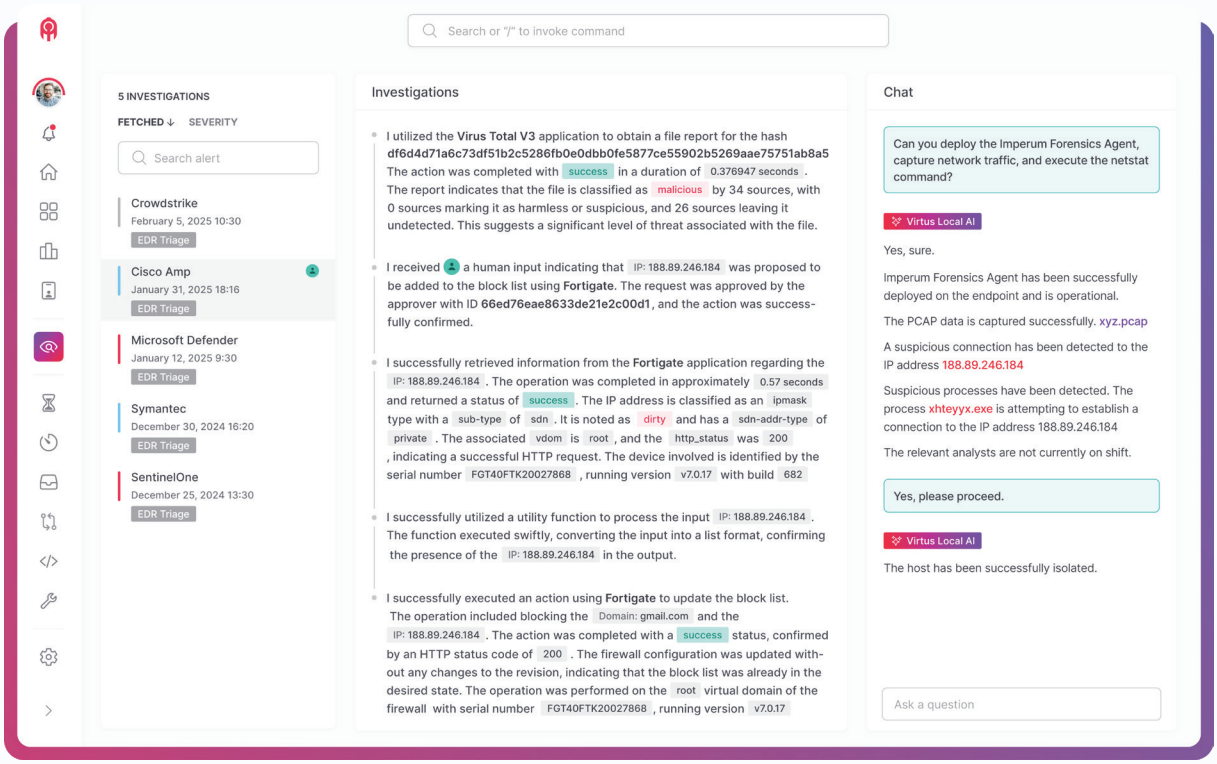
in efficiency, allowing teams to focus onhigher-value strategic threat hunting and remediation

**Investigation Coverage Expansion**

**3 times increase**

in coverage, ensuring no threat goes unchecked, reducing blind spots in security operations.

- **Alert Fatigue Reduction**
  *Fetches and processes data across your security ecosystem, vendor-agnostic and protocol-flexible.*
- **Hyperautomation**
  *Connects any technology, even legacy systems, via SSH, webhook, mail, Telnet, and more.*
- **Adaptive Decision-Making**
  *Executes response actions autonomously or escalates mission-critical cases.*
- **Human-in-the-Loop Collaboration**
  *ImperumMobile App enables analysts to validate findings and take action in real-time.*
- **Comprehensive Case Reporting**
  *Automatically generates detailed summaries and full investigation reports.*



# Why are we different?

- We alleviate the burden on SecOps teams by providing comprehensive, end-to-end support throughout the entire security operations life-cycle, enabling them to seamlessly ingest, analyze, hunt, and respond to threats within a fully integrated environment, ensuring optimal operational efficiency.
- We streamline complex GUIs, optimize orchestration, and leverage AI-powered Agents to close the expertise gap, ensuring no alerts are missed.
- We utilize machine learning to prioritize threats, provide real-time detection, automated analysis, and expanded visibility, all through a centralized security overview via a unified dashboard, seamlessly integrating with existing tools to maximize your current investment and enhance SecOps team efficiency.

# The value for you

**5x**

**More Affordable:** *Compared to traditional market solutions*
**Faster Implementation:** *Quick & seamless deployment*
**Less Vendors:** *Streamlined through supplier consolidation*
**Less Licenses:** *One license, all-inclusive*
**Less Subscriptions:** *Simple & transparent plan*

**Only Connector Agnostic Platform in the market**

Seamlessly integrate new technologies without writing a single line of code.

**Full Flexibility with On-Premise or Cloud**

Native Deployment for Seamless Integration.

**MTTD**

Reduce your Mean Time to Detect (MTTD) from weeks to hours, enabling faster and more efficient threat detection.

**600+ Collectors for Unmatched Forensics & Response**

Combine the comprehensive visibility of EDR with the robust response capabilities of DFIR.

**Connect Directly with Processes, Not Just REST APIs**

Whisper directly to the constraints of REST-API connections.

**MTTR**

Slash your Mean Time to Response (MTTR) from hours to minutes, ensuring rapid threat containment and remediation.

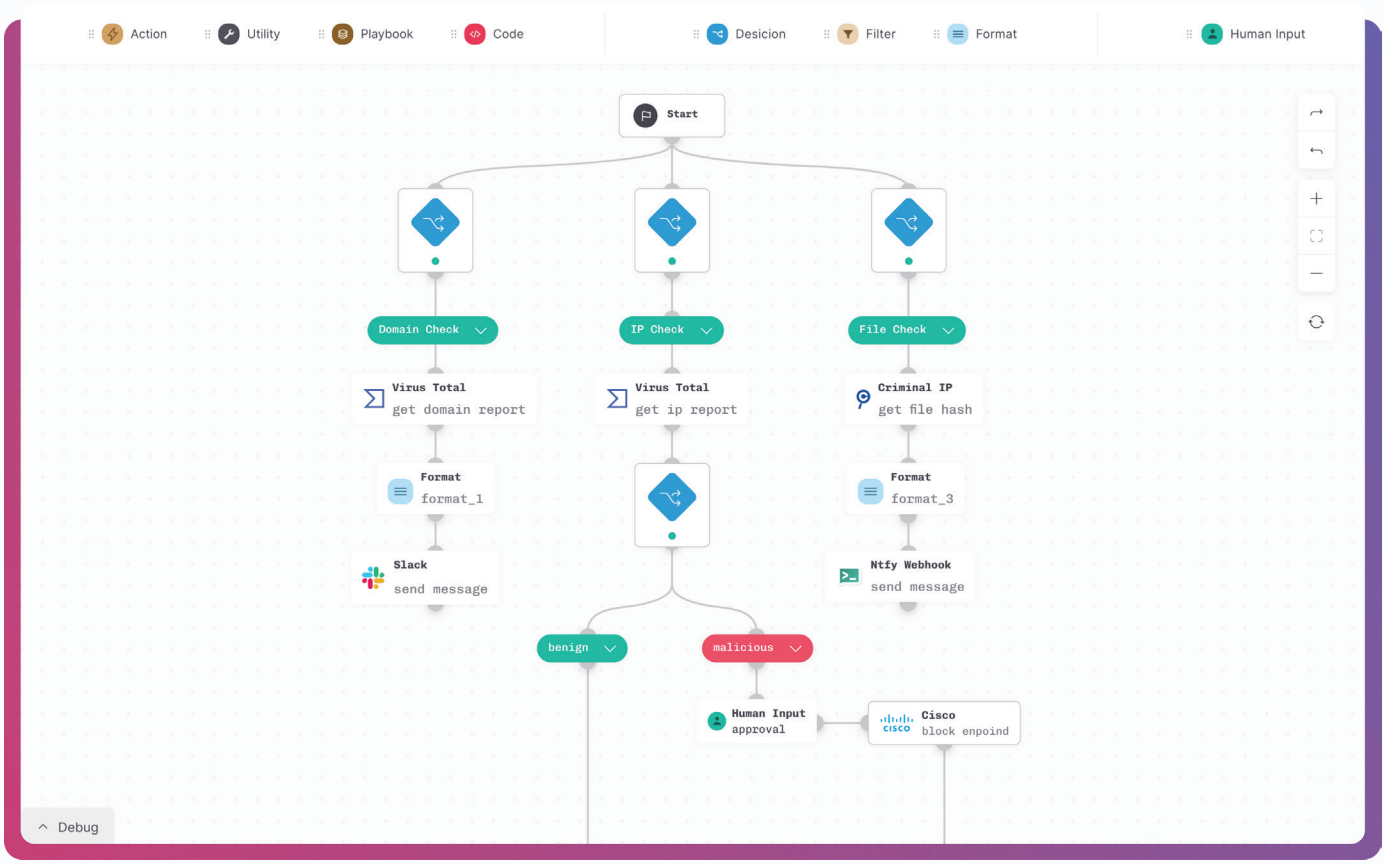
hyperautomation

# Experience the Power of No-Code SOAR with the Flexibility of Low-Code

## A game-changer in event processing and decision-making

With an intuitive drag-and-drop interface, you have the power to create an unlimited number of playbook runs quickly and easily, all without the need for any coding skills. This user-friendly system simplifies the process, allowing you to design and deploy complex workflows effortlessly, giving you complete control over your operations without the technical hassle.

The editor's versatility extends to its advanced data processing utility tool and the ability to run other playbooks within the current playbook. These features streamline your workflow and increase your productivity.




*With its built-in debugging capabilities, the editor ensures smooth and efficient playbook runs. It also allows low-code action insertions, giving you superior control over your playbook.*

## The only connector agnostic Hyperautomation: Integrate without manual coding

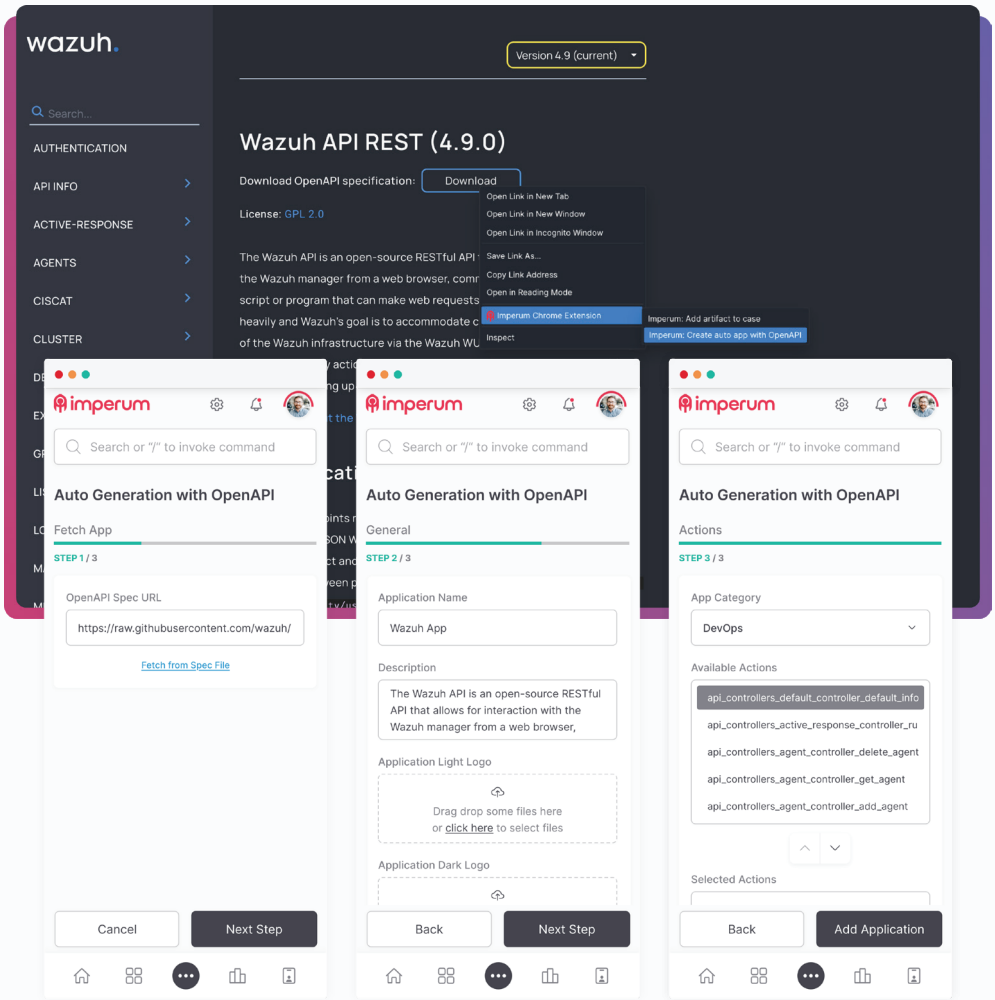
Our Hyperautomation is the only connector-agnostic SOAR in the market, allowing you to create custom REST-API connectors without any coding. We've solved the connector challenge with an AI-powered parser and coding platform, eliminating the need for lengthy integrations.

It lets you integrate any technology in just a few clicks. Plus, our Chrome extension lets you generate connectors in minutes, cutting down the time it would typically take by weeks.

# Imperum App Connector Wizard

We invested significant time and engineering expertise to resolve this challenge. By creating an AI-powered parser and coding platform, we completely eliminated the connector issue.

This empowers customers to build their own REST-API connectors for their solutions independently, without needing our support or manually writing any code.

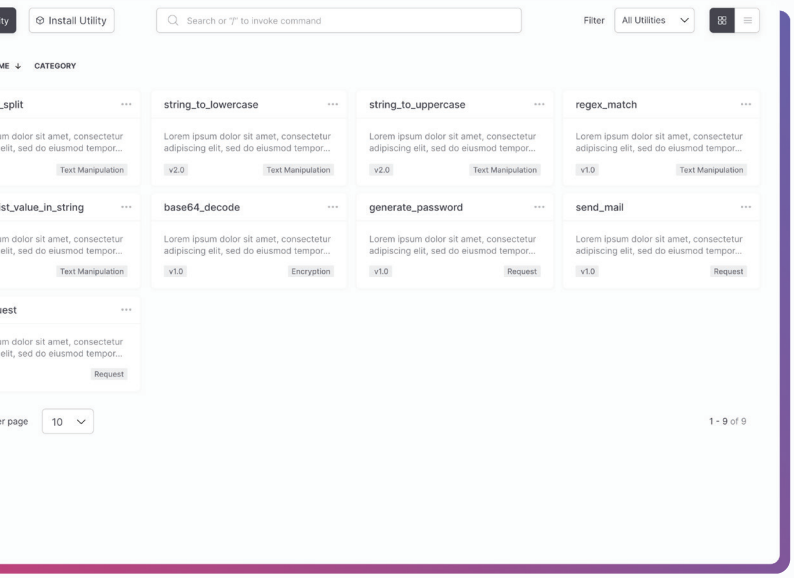


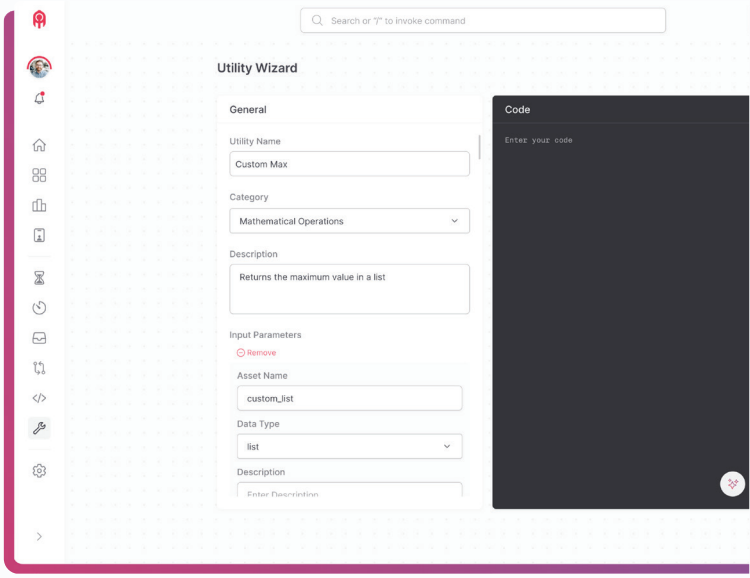
# AI-Powered Utilities:

## Seamless Integration Beyond REST APIs

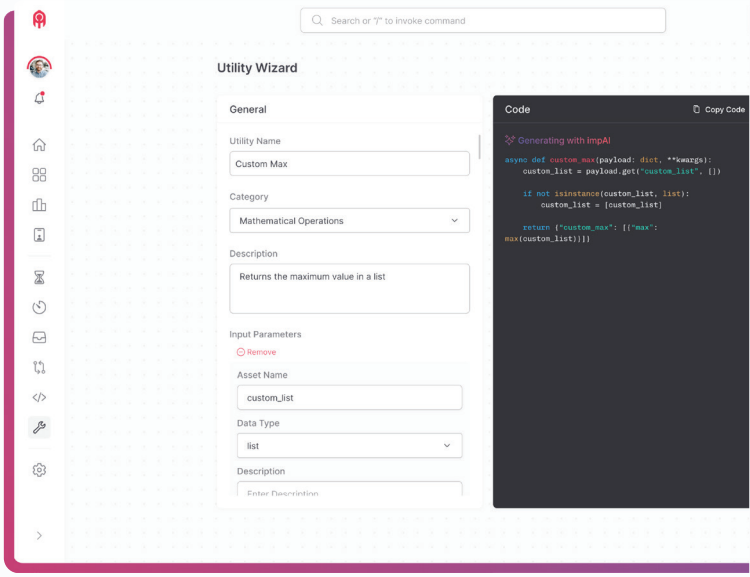
In today's complex tech landscape, not all technologies support REST APIs, creating challenges for organizations looking for smooth integrations.

Our AI-powered Utilities feature bridges this gap effortlessly. It integrates with a wide range of protocols-including Telnet, SSH, RDP, Webhooks and CLI-without the need for any coding.




*This unique solution, unmatched by any other SecOps platform in the market, enables you to connect with legacy systems and technologies that don't support modern API standards, ensuring operational efficiency and compatibility across your entire tech ecosystem.*

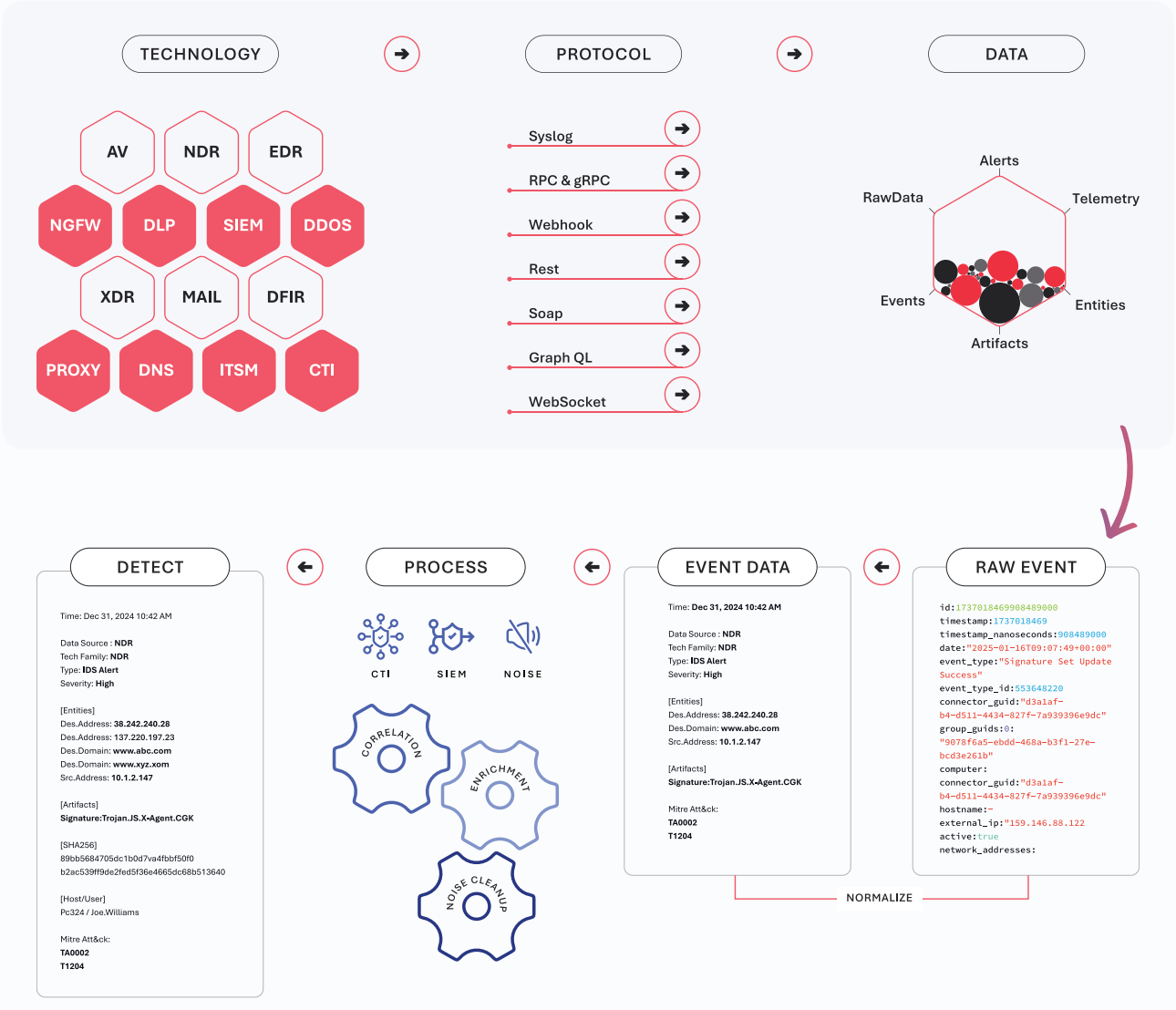


ingest

# Seamless Ingestion or Complete Security Visibility

Imperum's Ingest module seamlessly collects events, alerts, IOAs, and IOCs from a wide range of security technologies NGFW, DLP, SIEM, DDoS, ITSM, CTI, and more using multiple protocols like Syslog, REST, GraphQL, Webhooks, RPC/gRPC, Websockets, and SOAP.

It normalizes raw data into structured event data, applying correlation, enrichment, and noise reduction to eliminate false positives and enhance security insights. With Imperum, you get clean, enriched, and actionable data for faster detection and response all in real time.



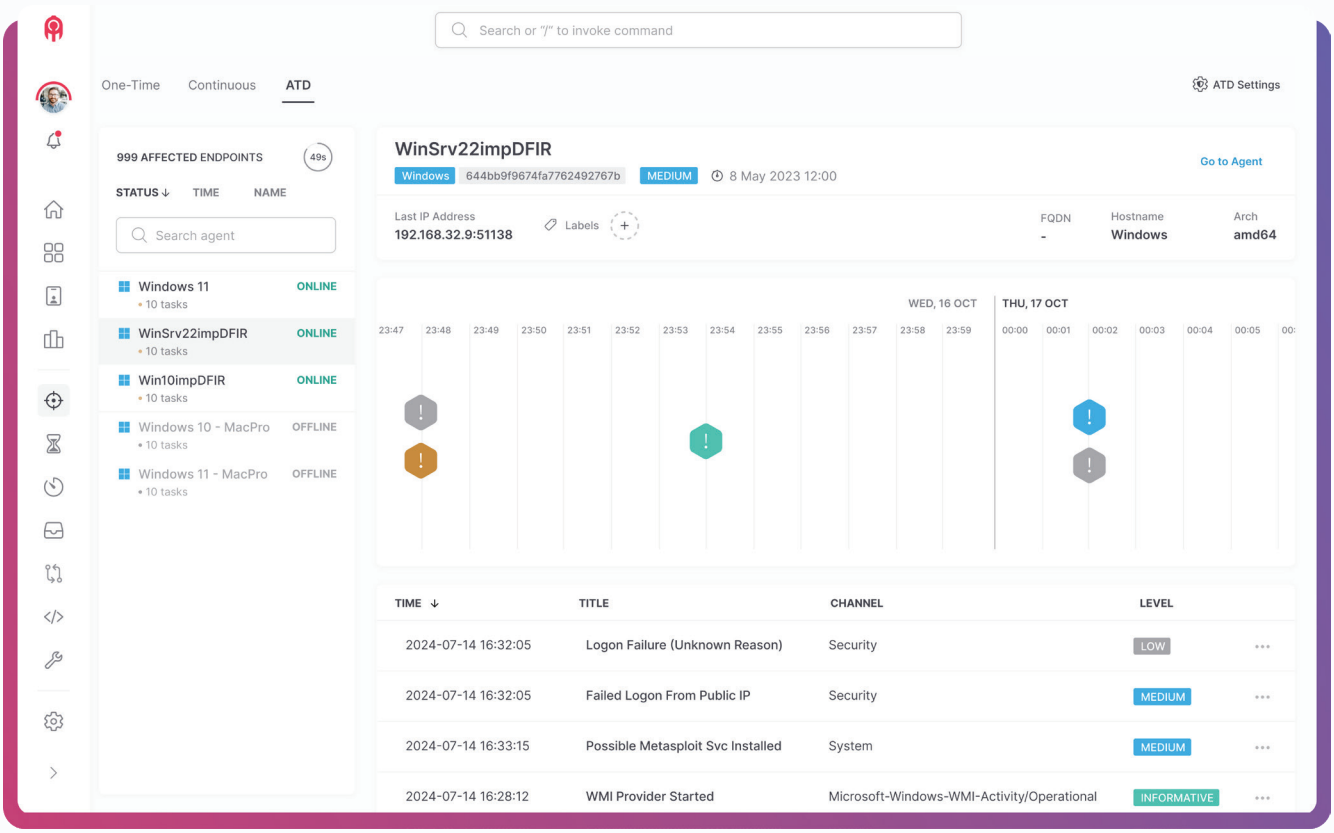
detect

# Stop Threats Before They Escalate

Our Advanced Threat Detection capability seamlessly integrates endpoint detection with digital forensics, leveraging SIGMA rules to identify and neutralize threats in real-time.

Our AI-driven automation enables instant forensic analysis through dynamic playbooks, eliminating manual complexity and accelerating incident response.

*This isn't just detection - It's proactive, intelligent defense designed to stop threats before they escalate.*

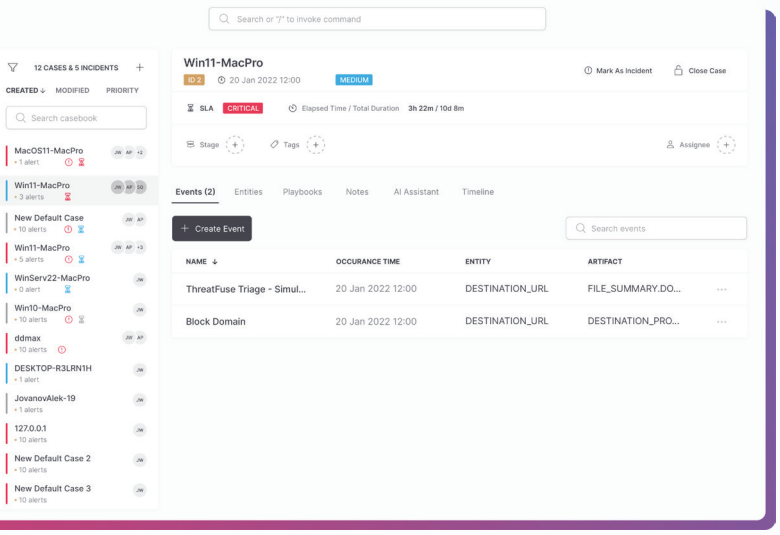


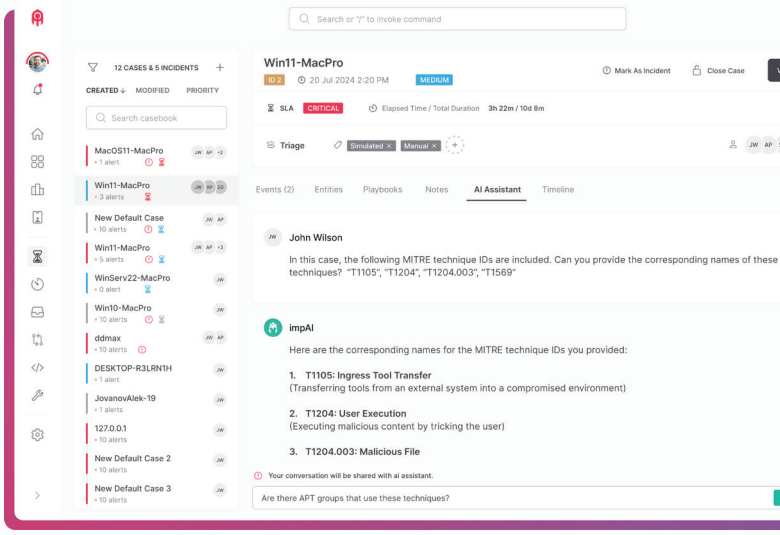
# AI-Driven Casebook - Unleash the Power of Our Comprehensive Incident Management Platform:

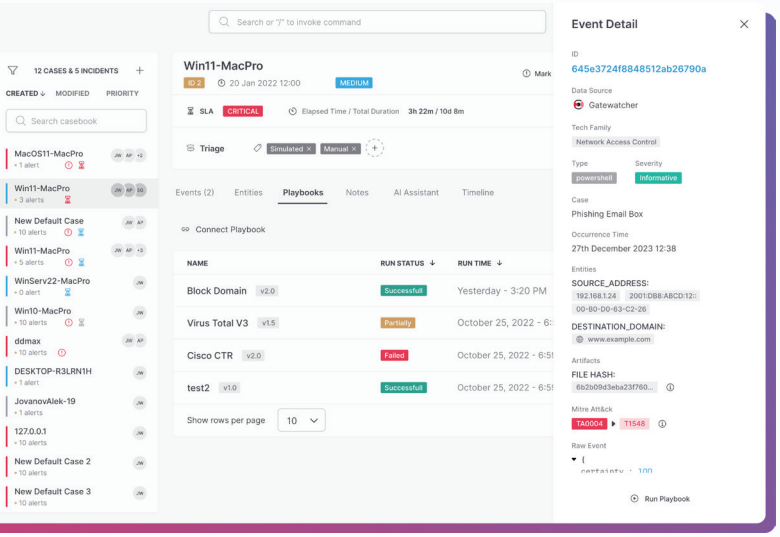
## Your Essential Ally for Operational Stability

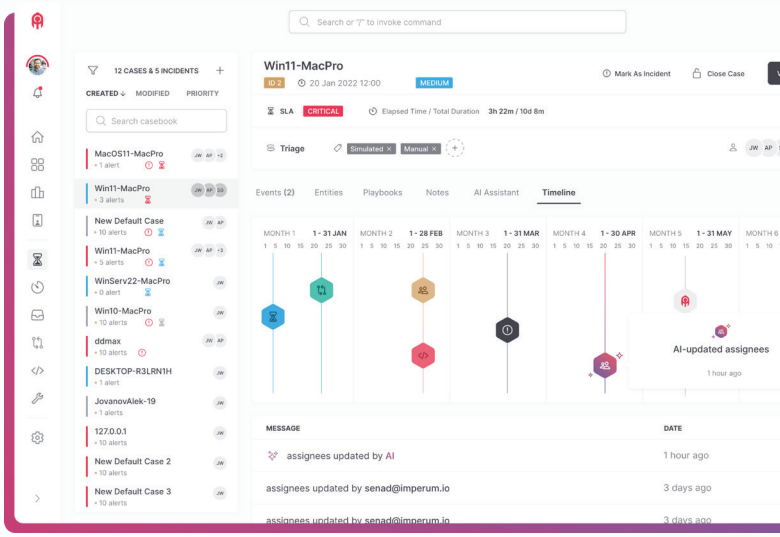
Analysts rely on SOAR, threat hunters demand XDR, and responders depend on DFIR. At Imperum, we bring all these essential capabilities together within our Casebook IR platform, offering a unified interface for seamless and efficient cybersecurity operations.

Our platform includes a powerful, feature-rich Casebook, allowing you to generate unlimited cases-both manually and automatically, acting as a comprehensive library of past incidents. The Casebook enables retrospective analysis, helping you identify patterns and trends to enhance future incident management.



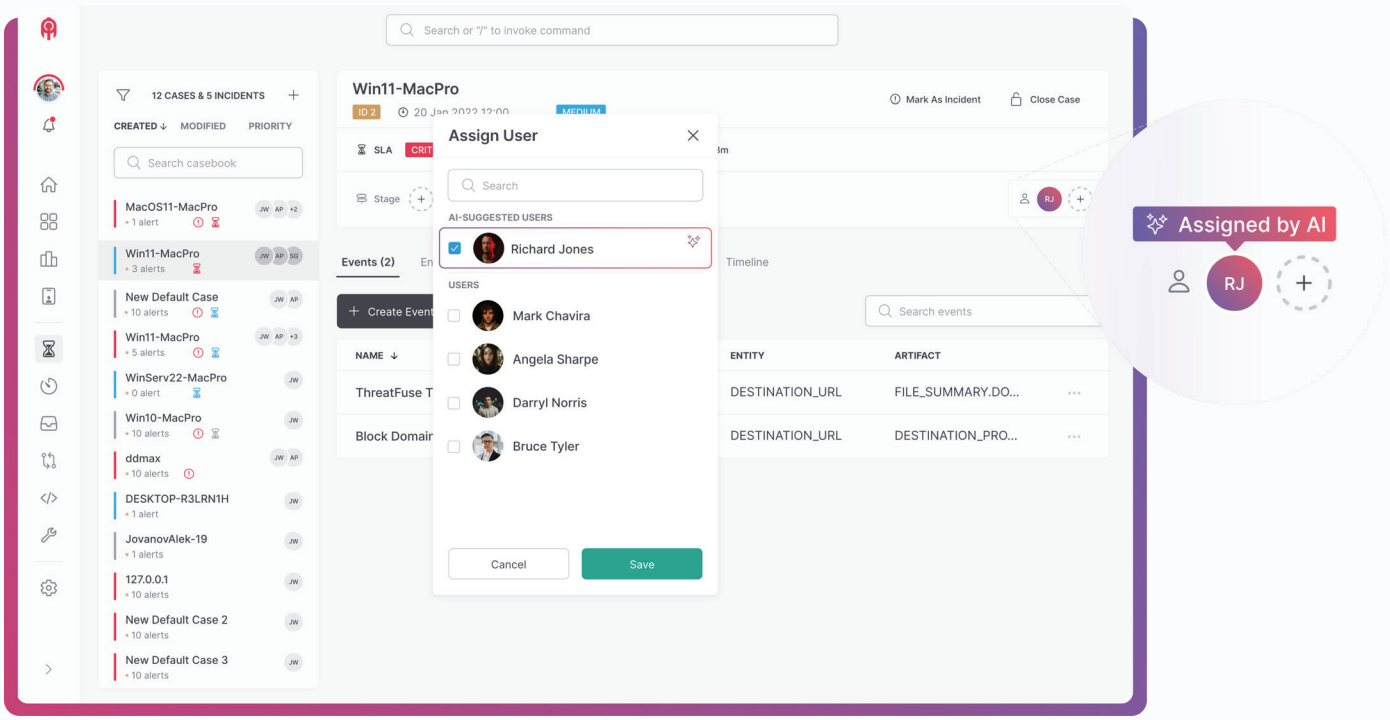

*With this tool, you can effectively prioritize cases and ensure that no critical incident is ever overlooked.*

# AI-Powered Auto Case Assignment:

## Smarter, More Efficient Security Operations

Our localized trained AI model boosts the efficiency of your security teams with the **AI-Powered Auto Case Assignment** feature, a cutting-edge, air-gapped solution.

This intelligent system continuously learns from your SecOps team's behaviors and incident handling patterns, evolving to understand how each case is best managed. By automatically assigning cases to the most suitable analysts based on their unique strengths and past performance, it ensures that every incident is handled by the right expert.



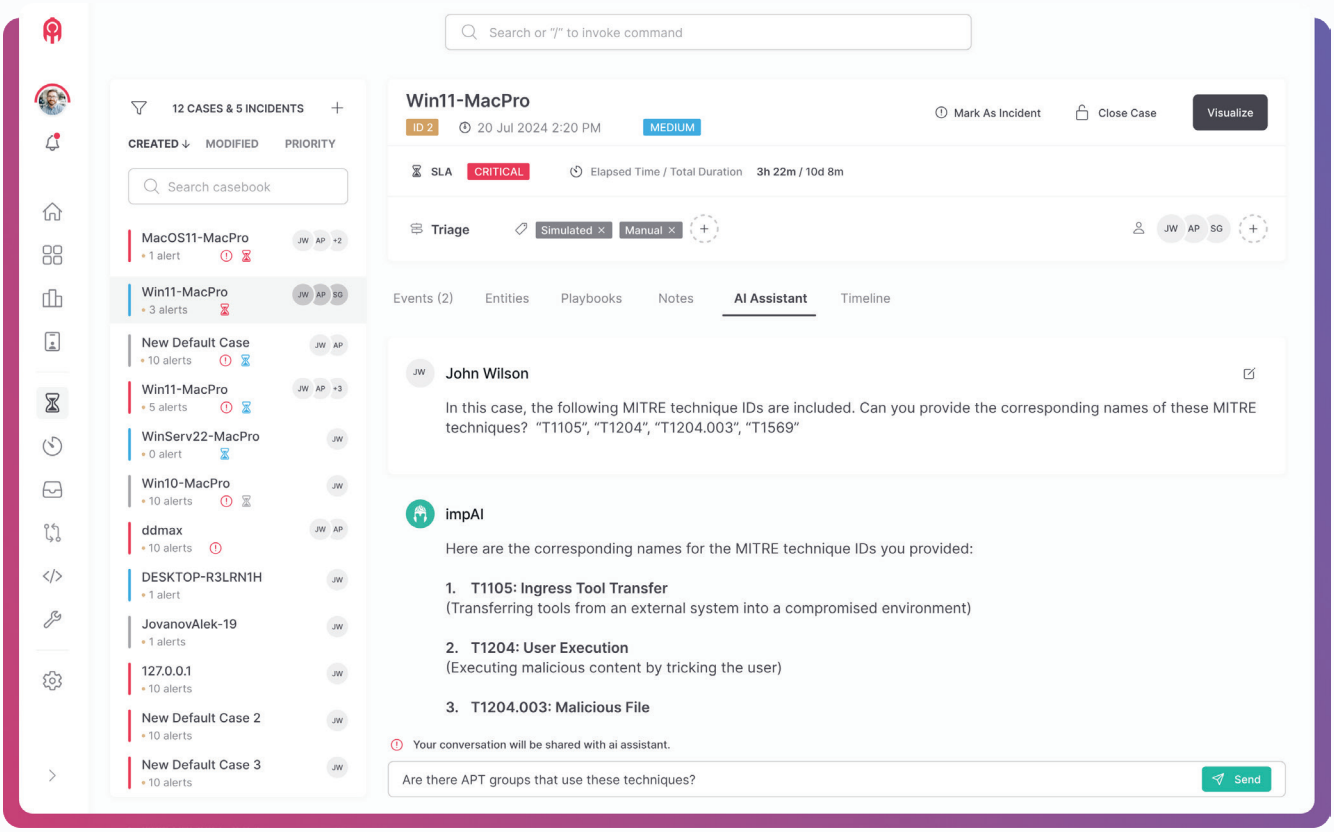

This optimized case allocation not only leads to faster incident resolution but also maximizes resource management, allowing your team to focus on what matters most:

## Keeping Your Organization Secure

# AI-Powered Virtual Analyst & Responder Agent:

## Augmenting your SecOps Team for Faster, Smarter Incident Response

Introducing a game-changing feature designed to supercharge your SecOps team's capabilities: the AI-Powered Virtual Analyst and Responder Agent.



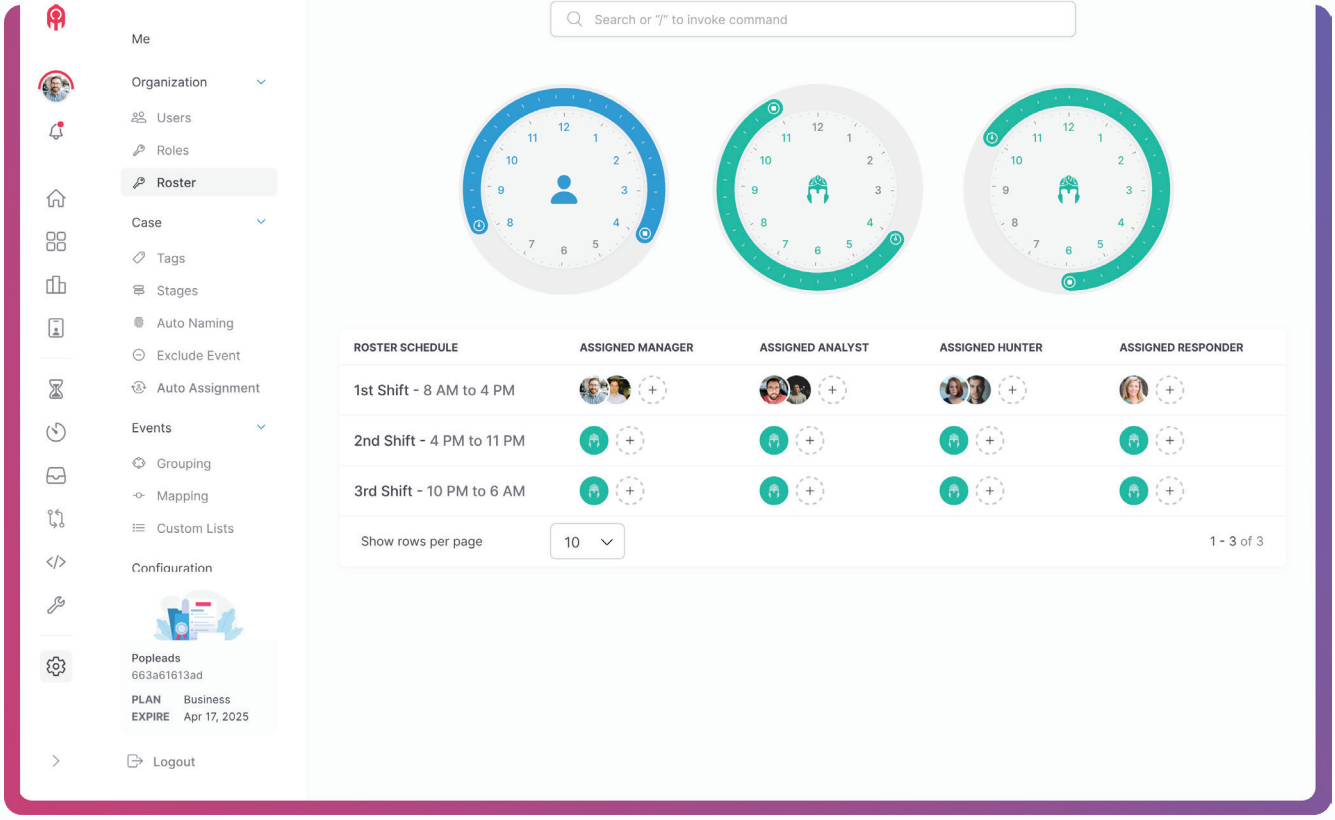

*Your team can leverage the AI agent to quickly define alerts by requesting relevant information about incidents.*

*This intelligent virtual assistant enhances incident management and significantly reduces response times by seamlessly integrating with your security operations.*

Additionally, it empowers your SecOps team to take immediate action by automating critical tasks, such as isolating compromised hosts and blocking malicious source IPs. With the Virtual Analyst and Responder Agent, your team is always ready to respond faster and more effectively, ensuring optimal security outcomes.

# AI-Driven SecOps Roster Agent: 24/7 Ensuring Operational Efficiency

Maximize the efficiency of your security operations with our **AI-Driven SecOps Roster Agent**, a unique feature that allows you to seamlessly manage human and virtual shifts. With this intelligent scheduling tool, you can effortlessly assign shifts for your human analysts while designating specific periods for virtual analysts and responder agents to take control.

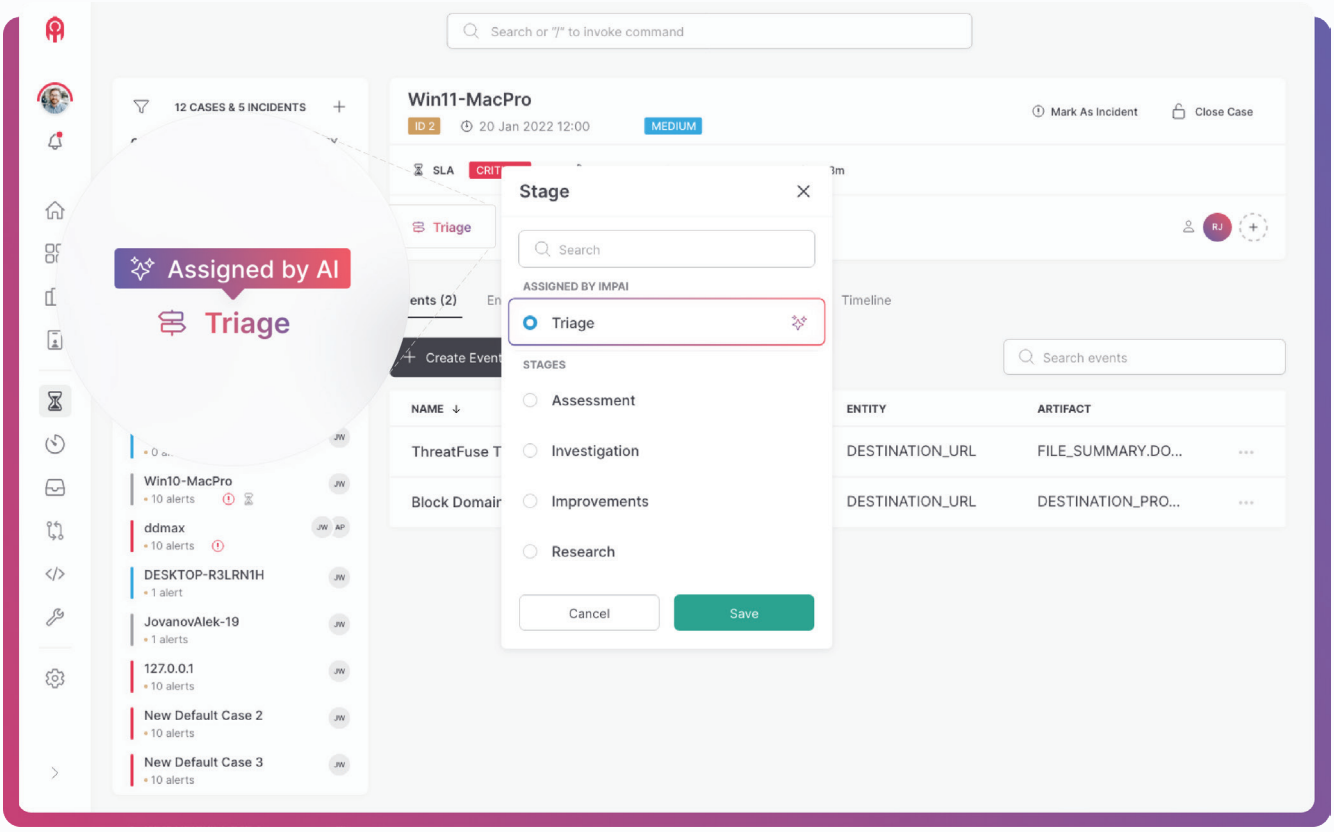



This flexible, hybrid setup ensures that your security operations are fully staffed around the clock, maintaining peak effectiveness at all times. Whether it's covering off-hours or managing high demand periods, the **AI-Driven SecOps Roster Agent** guarantees that your team operates at its best, 24/7.

# AI-Powered Auto Triage Agent:

## Rapid, Accurate Incident Management for Faster Responses

Our **AI-Powered Auto Triage Agent** is a revolutionary feature designed to streamline incident response by quickly and accurately evaluating the severity and nature of security events as they occur. This intelligent agent prioritizes cases based on the level of threat and potential impact, ensuring that the most critical incidents are addressed first.




By automating and enhancing the triage process, this feature accelerates decision-making, significantly reducing response times and minimizing risk to your organization. With the **AI-Powered Auto Triage Agent**, your SecOps team can focus on resolving the most pressing threats, maintaining operational security, and reducing the overall threat landscape.

forensics

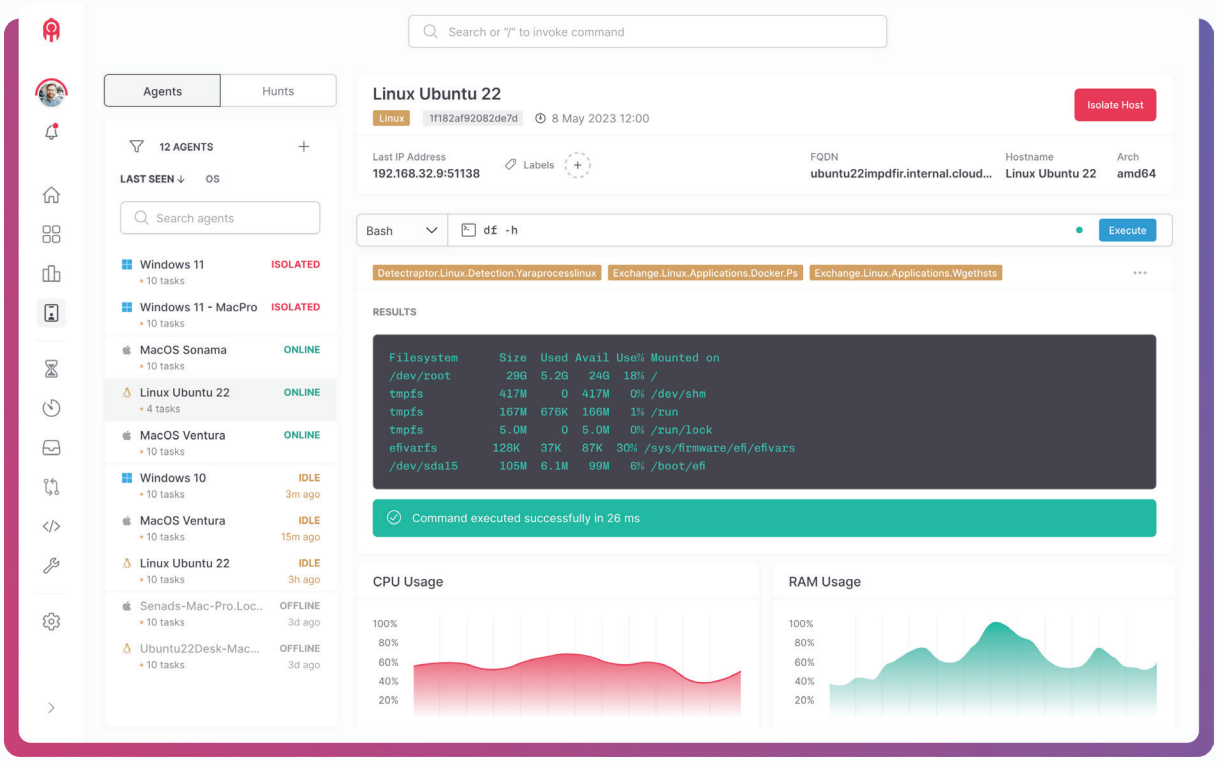
# Harness the Power of 600+ Predefined Artifact Collectors for Unmatched Digital Forensics and Incident Response

The **Forensics** module is a revolutionary tool that combines the comprehensive visibility of EDR with the robust response capabilities of DFIR. With **Forensics**, the complexities of data breaches become manageable, allowing faster and more efficient investigations.

What truly sets **Forensics** apart is its extensive library of over 600 predefined, community-powered artifact collectors-the only DFIR solution on the market with such breadth and power. These collectors provide unparalleled insight into security incidents, enabling your team to tackle even the most intricate breaches precisely and easily.

Also some facts in numbers:

- **600+ Community Supported Artifacts**
- **Compatibility with:**
- **Agentless Collection**
- **Built-in Host-Isolate Function**
- **Microscopic Forensics Capability**
- **Full Remote Bash & PowerShell Access**

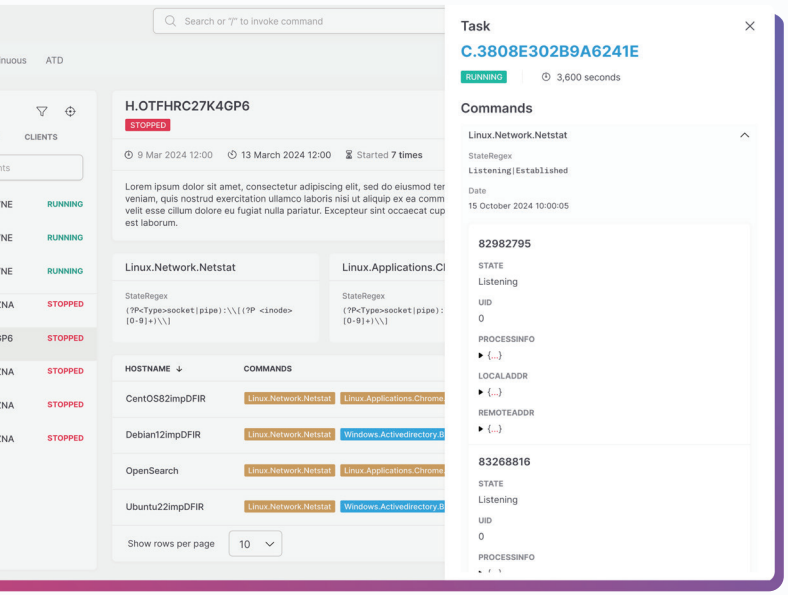


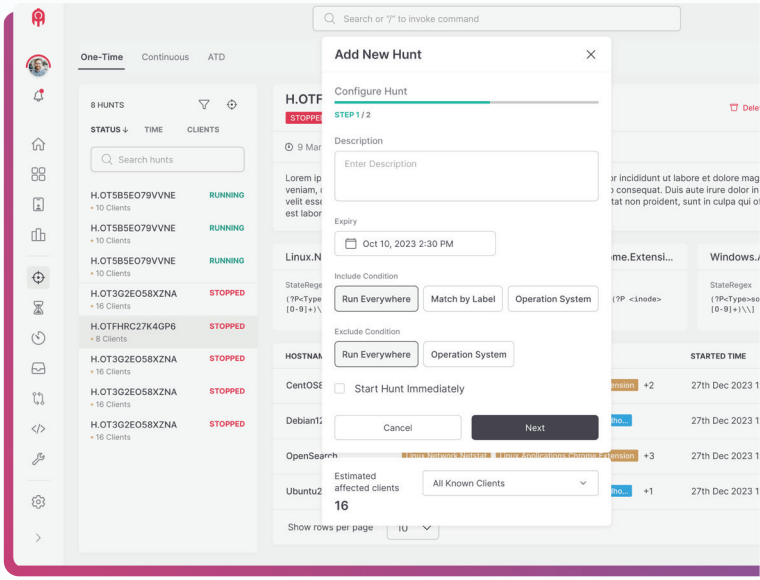
# On-Demand Threat Hunting

## Forensic Analysis for Hidden Threats

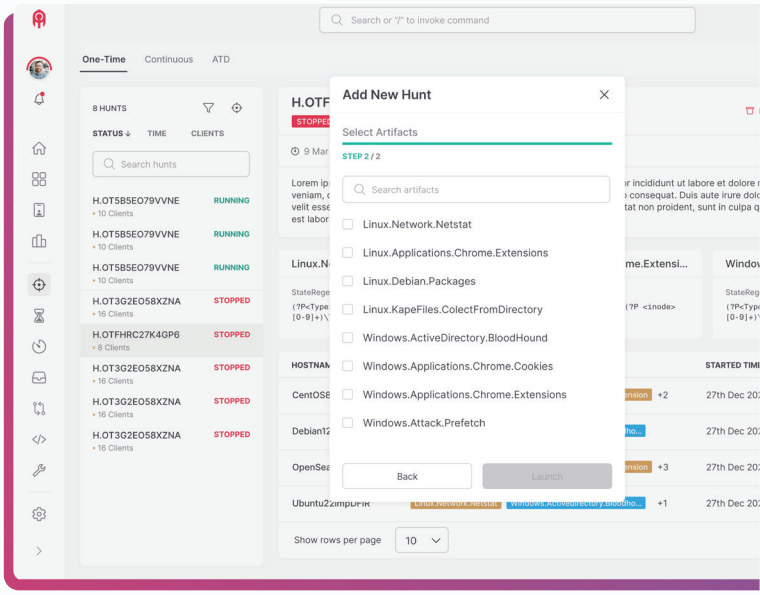
The **On-Demand Threat Hunting** is a powerful, on-demand threat-hunting feature available exclusively in **Forensics**. This function allows your security team to actively search for hidden threats in real time, bypassing conventional detection methods that often miss more sophisticated attacks.

*Utilizing advanced behavior analysis, the On-Demand Threat Hunting identifies malicious activity that goes undetected by standard alarms.*




*It provides your team with the ability to conduct comprehensive, one-time threat hunts across all major operating systems, including Windows, Linux, and macOS, ensuring no threat slips through the cracks.*




With this unique feature **Forensics** equips your organization to proactively uncover and neutralize potential risks before they escalate, offering unparalleled control over your cybersecurity defenses.

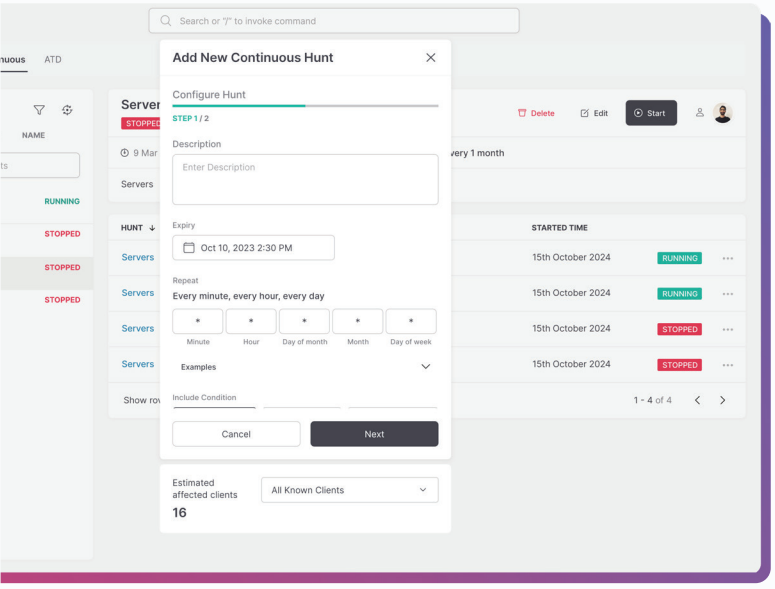
# Continuous APT Hunter:

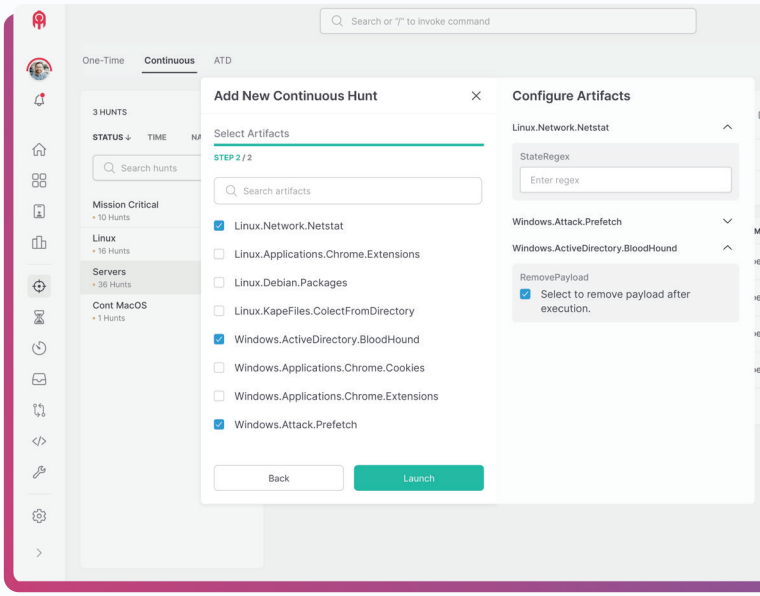
## Uncover Hidden Advanced Persistent Threats with APT Hunter

The **Continuous APT Hunter** is a standard feature within **Forensics**, designed to actively detect and mitigate Advanced Persistent Threats (APTs) that often evade traditional detection methods. By focusing on behavioral analysis, this powerful tool identifies threats that do not trigger conventional alarms, uncovering the subtle patterns and behaviors associated with APTs.

With the **Continuous APT Hunter**, you can set up periodic threat hunts targeting specific servers or endpoints, scanning for key APT behaviors such as:

- **Startup items**
  *identifying persistence mechanisms*
- **Logged-in users**
  *detecting backdoor access*
- **Artifacts**
  *323* *87* *48*
- **Netstat**
  *monitoring for new listening ports*
- **And 600+ additional behavioral patterns**




*This feature ensures your organization is equipped to continuously detect and respond to APTs, giving you proactive, round-the-clock protection against sophisticated, hidden threats.*

# Automated Investigation & Response

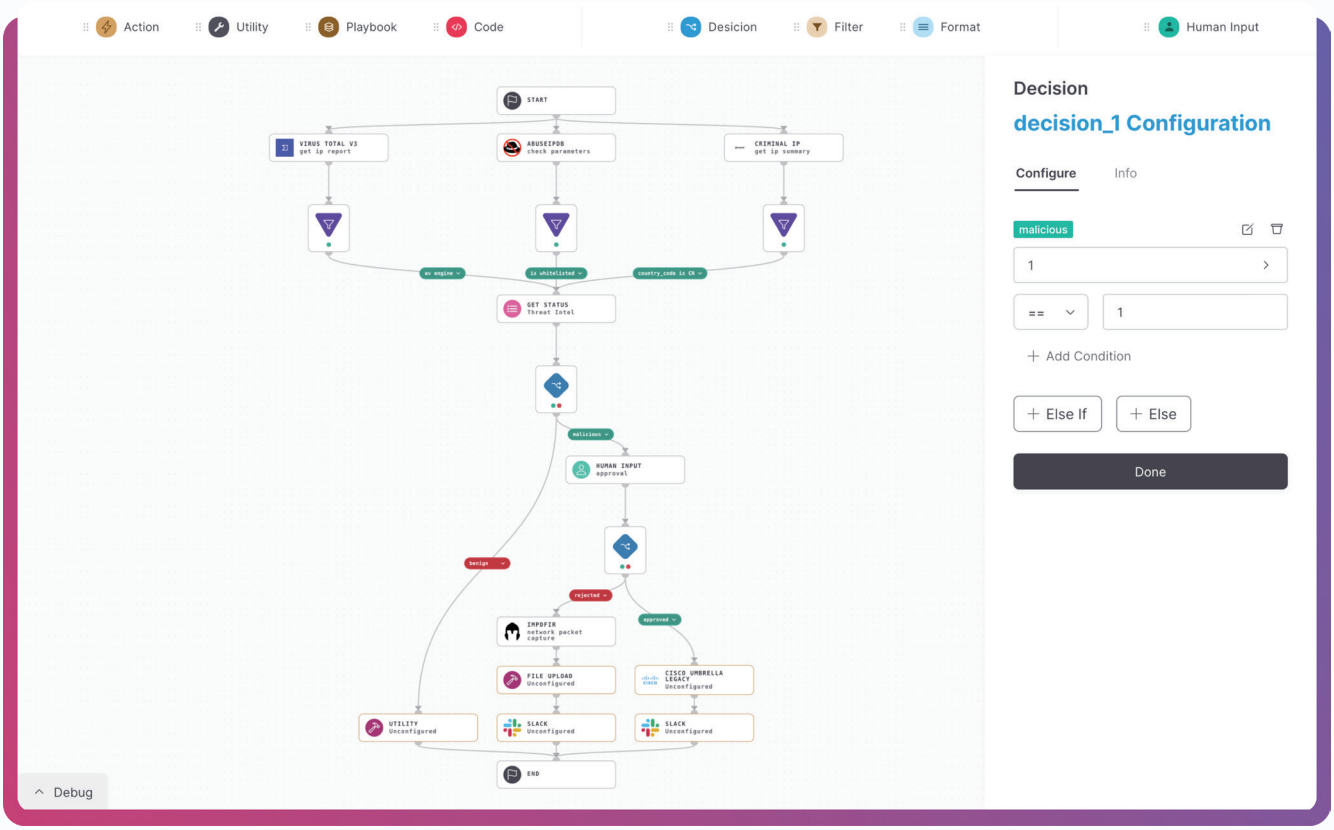
## Communicate Directly with Processes, Not Just REST-APIs

Our groundbreaking solution allows you to interact directly with processes, bypassing the limitations of REST-API connections, using the powerful combination of our **Hyperautomation** and **Forensics** modules.

This award-winning capability is integrated within the playbooks, empowering your security teams like never before.

With **Forensics** and **Hyperautomation**, you can fully automate Digital Forensics and Incident Response (DFIR) tasks through customizable, automated playbooks. This unique functionality provides responders with the ability to craft specialized workflows tailored to their specific forensic needs, simplifying complex investigations and incident response activities.

forensics ⇄ hyperautomation



imperum

Mobile App


Coming Soon

# Not Convinced Yet? Security at Your Fingertips Anytime, Anywhere

We know how crucial it is to stay in control of your security and respond to threats in real-time. That's why we developed our mobile app putting all your alerts and open cases directly on your phone, so you can take immediate action wherever you are.

Seamlessly integrated with your security environment, it empowers you to respond quickly and effectively, ensuring your organization remains protected 24/7.

# We're Here To Help

We at IMPERUM are dedicated to providing exceptional customer service and ensuring that you are satisfied with our product. If you have any questions, comments, or concerns, please do not hesitate to contact us.

## Request a Demo

Are you keen to explore how IMPERUM could enhance your cybersecurity framework?

Simply click the button below and complete the form. Our team of cybersecurity professionals will promptly get in touch to initiate your transformation journey!

Request a Demo

## Office

**Europe, HQ**
Teleport Towers, Kingsfordweg 151, 1043 GR, Amsterdam, NL

**USA, Office**
8 The Green #12517, Dover, DE 19901

## Customer Support

For immediate assistance with our product or any technical issues, please email our customer support team:

support@imperum.io

Our customer service team is available 24/7 and typically responds within 24 hours.

## For More Information

www.imperum.io

## Sales Inquiries

Interested in purchasing IMPERUM or have questions about pricing? Please reach out to our sales team:

sales@imperum.io