

ACS Tools Presentation

Sebastien PEYNET – *Project Manager*
Airbus CyberSecurity

January, 23th 2025



This project has received funding from the European Union's Horizon Europe research and innovation programme under Grant Agreement No 101120779 .

Summary

- 1 Cyber Range**
ACS
- 2 SIEM - GrayLog**
ACS
- 3 SOAR – ProheCy**
ACS
- 4 Q&A**
Audience

CyberRange

a platform that can **simulate** highly sophisticated and **realistic** environments

Exercises, Training and Education



Operational Tests and Validation



Reproduce **realistic complex systems** (IT, OT and SCADA)

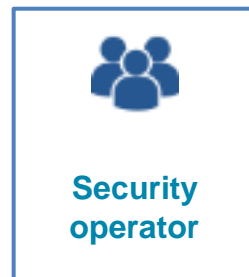
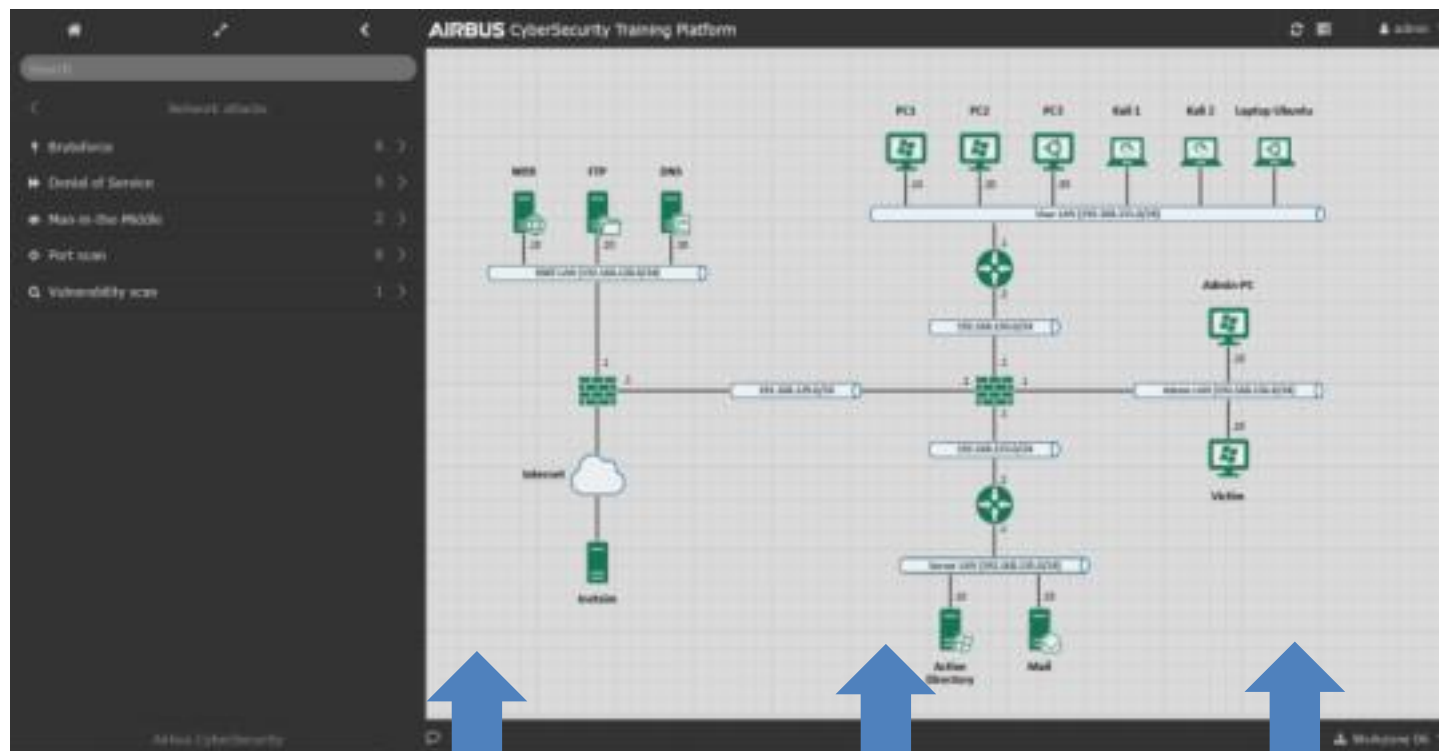
Content Library provided

Customised content

Hybrid capacity:
interconnection with your existing HW&SW systems

Physical or **SaaS**

CyberRange Exercises



Log management

NIST summary helps to identify objectives and process to be put in place:

- “Organizations should establish policies and procedures for log management.”
- “Organizations should establish standard log management operational processes:
- Monitoring the logging status of all log sources
- Monitoring log rotation and archival processes
- Checking for upgrades and patches to logging software, and acquiring, testing, and deploying them
- Ensuring that each logging host’s clock is synched to a common time source
- Reconfiguring logging as needed based on policy changes, technology changes, and other factors
- Documenting and reporting anomalies in log settings, configurations, and processes.”.

SIEM basics

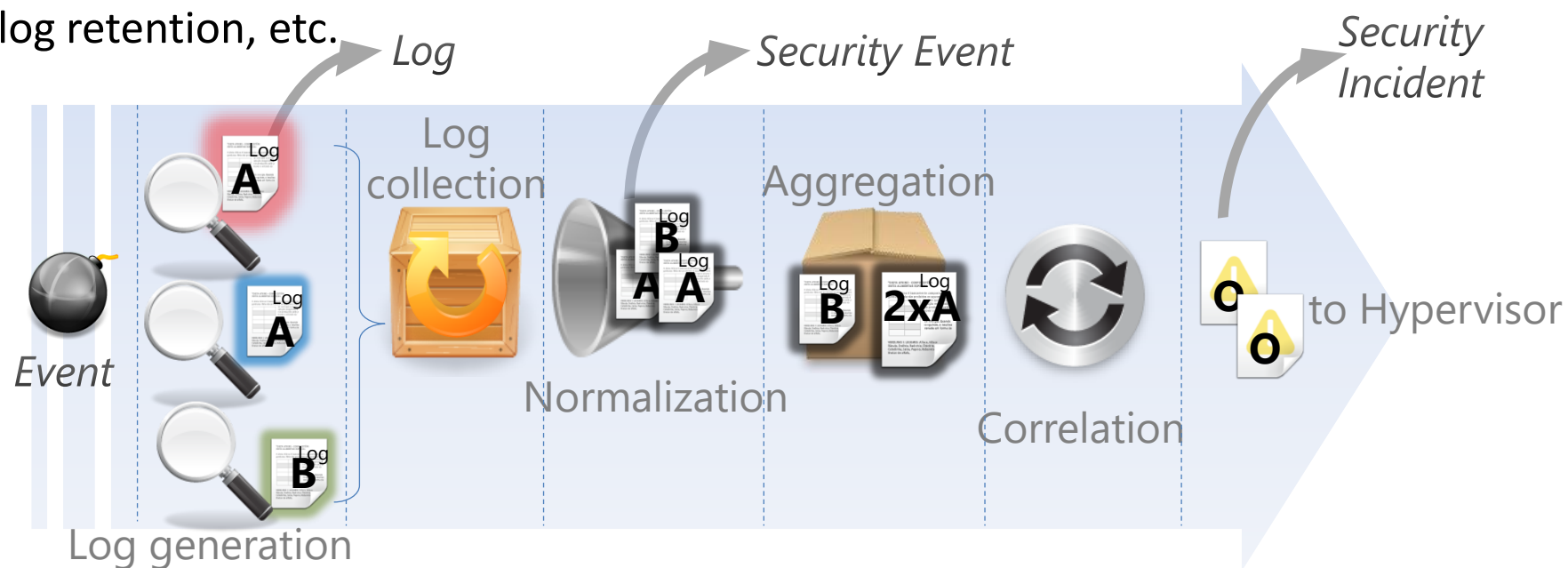
The SIEM product family is the core of events and information management. SIEM are providing security information management and also event management, by collecting information system logs from multiple assets and managing security event in real-time. Main commons features of SIEM products are:

Log collection and forward to Log manager

Log parsing, aggregation, normalization and correlation

Data indexing for query, reports visualization and analysis.

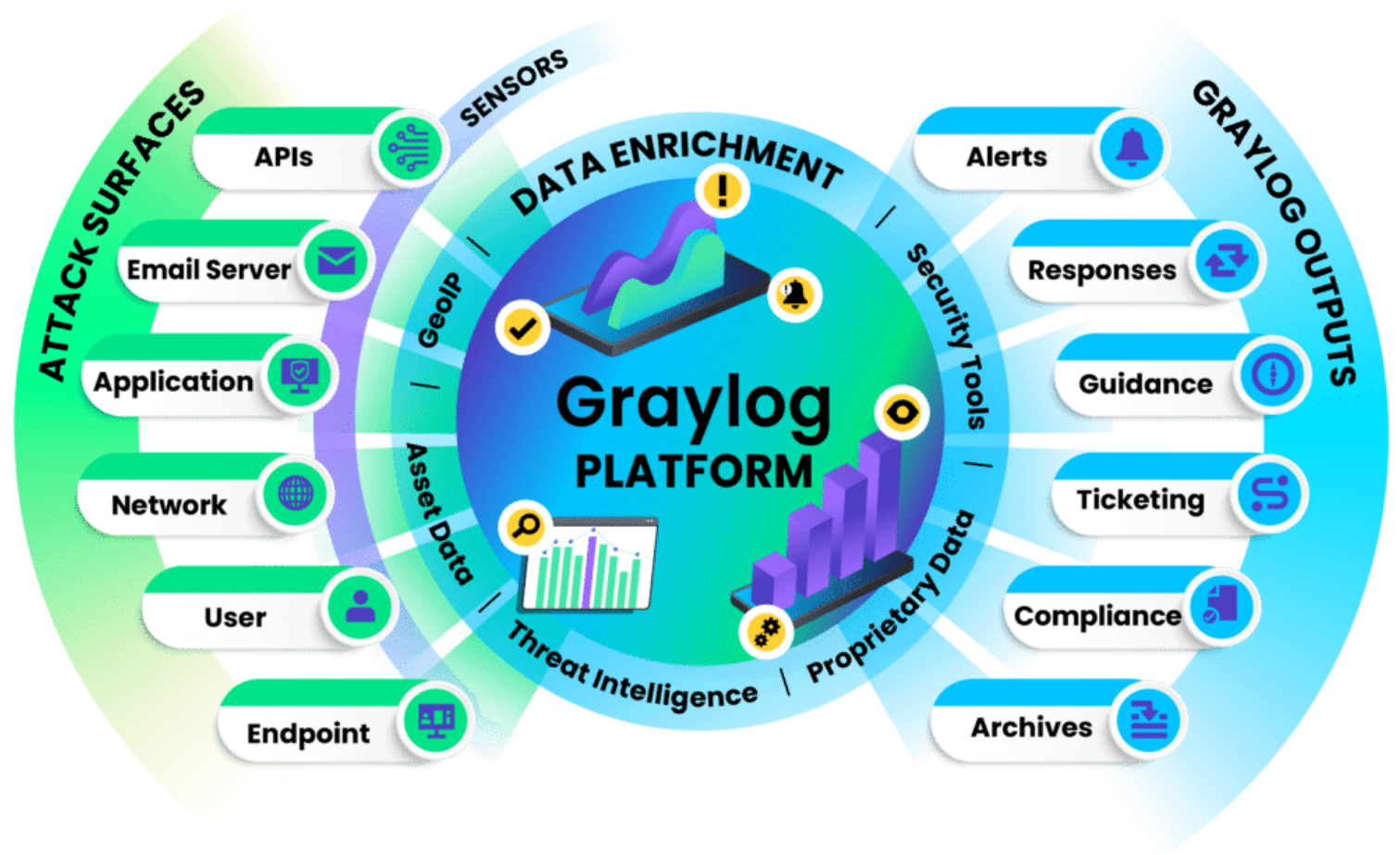
Depending of editor, SIEM products offers the toolbox for incident handling with real time alerting, forensic capabilities with log retention, etc.



SIEM - Graylog

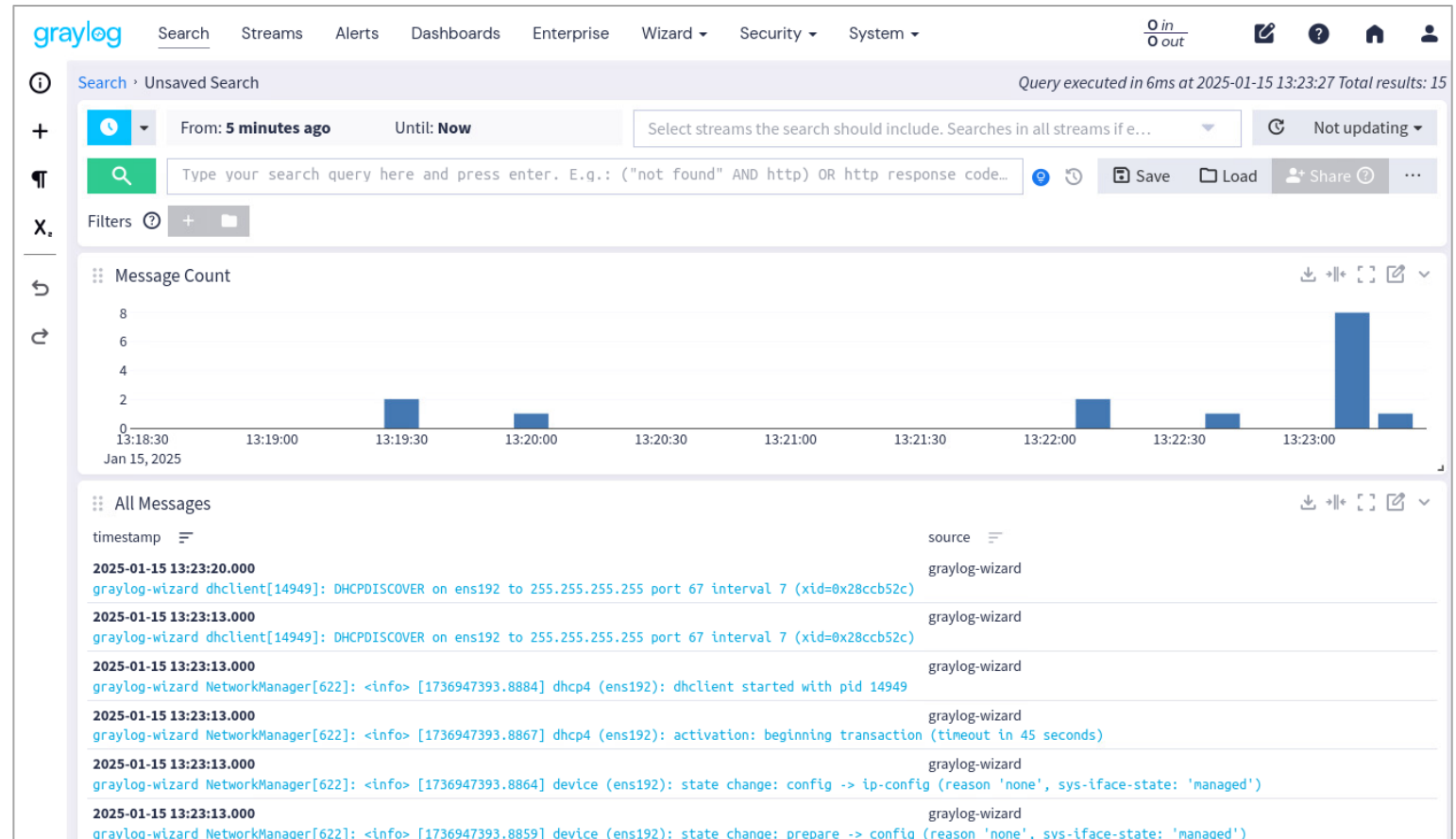
Log management solution :

- Log data aggregation
- Log data analysis
- Log data management



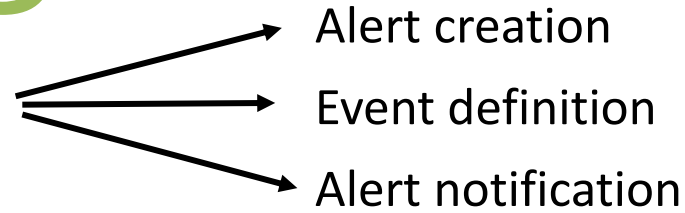
SIEM - Graylog

- Unlimited log ingestion
- View log data in real-time
- Search through volume of log data
- Configure alerts for what matters most



Graylog Wizard

Plugin to manage the alert rules



Alert Rules

With the wizard, you can manage the alert rules. An alert rule consists of one or more streams with rules, an alert condition and an alert notification. Read more about Wizard alert rules in the documentation (wizard version : 6.1.0).

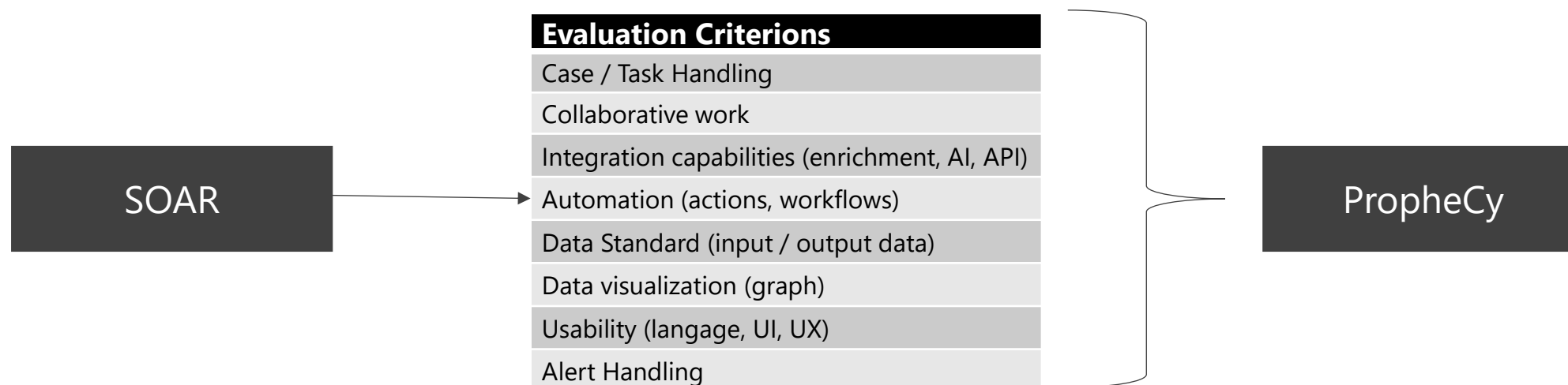
Filter alert rules

Bulk actions

<input type="checkbox"/> Title	Priority	Description	Created	Last Modified	User	Status	Actions
<input type="checkbox"/> aaa	High		2024-12-24 09:09:58	2024-12-24 09:44:17	admin	Disabled	<input type="button" value="▶"/> Edit Event definition Notification Clone
<input type="checkbox"/> bbb	Low		2024-12-24 09:30:41	2024-12-24 09:30:41	admin	Enabled	<input type="button" value="▶"/> Edit Event definition Notification Clone
<input type="checkbox"/> rrr	Low		2024-12-24 10:08:09	2024-12-24 10:08:09	admin	Enabled	<input type="button" value="▶"/> Edit Event definition Notification Clone
<input type="checkbox"/> aaa2	High		2024-12-24 10:12:20	2024-12-24 10:12:20	admin	Disabled	<input type="button" value="▶"/> Edit Event definition Notification Clone
<input type="checkbox"/> issue 101	Low		2025-01-07 16:07:22	2025-01-07 16:07:22	admin	Enabled	<input type="button" value="▶"/> Edit Event definition Notification Clone

Tools for Incident Response

Security Orchestration Automation and Response (SOAR) => a centralized and more efficient approach for incident response.

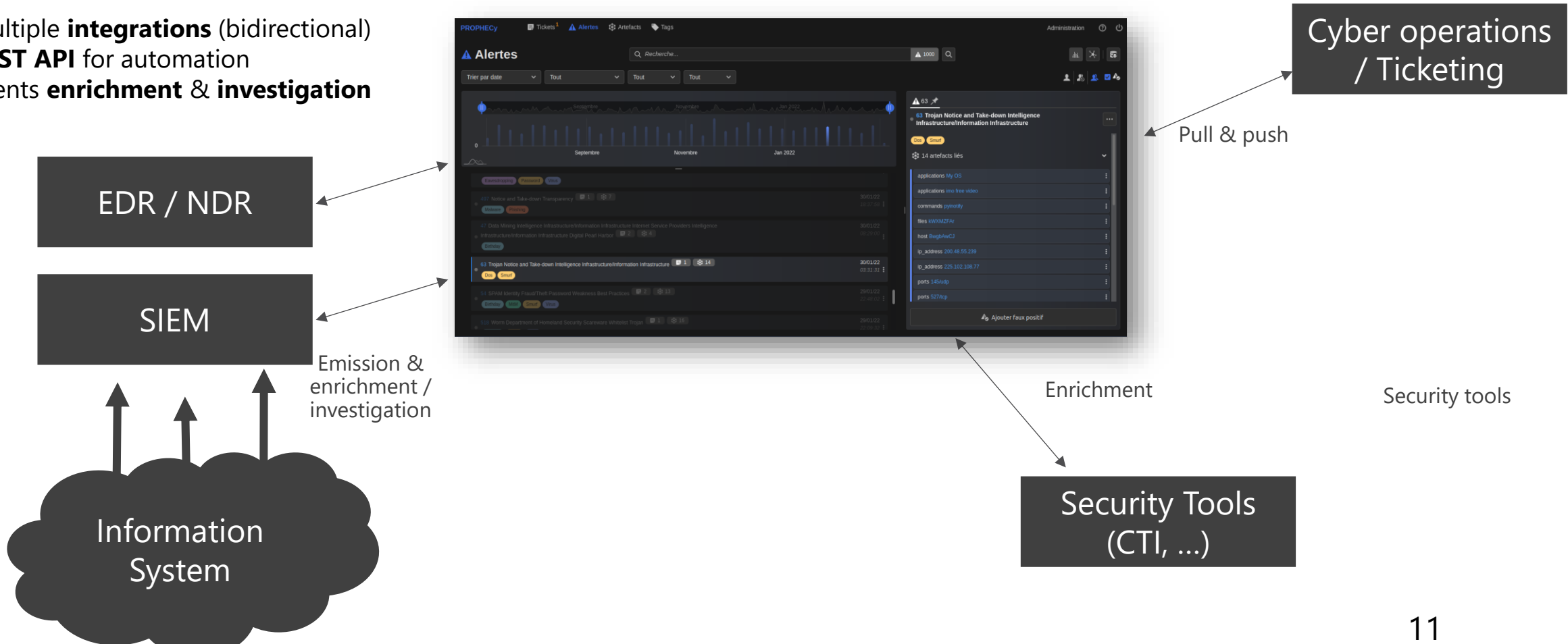


Introducing

PROPHECy

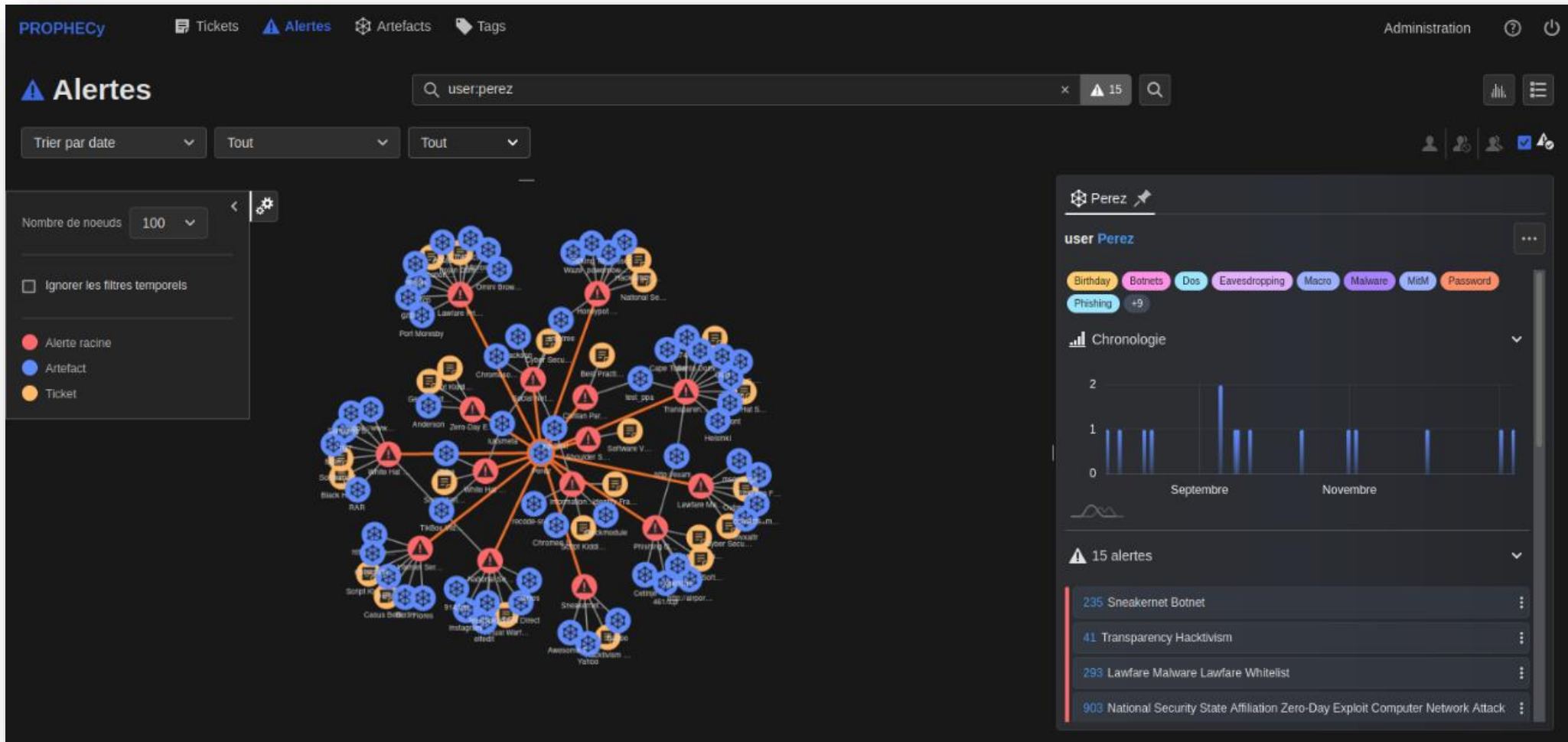
Visualize - Understand - Automate

- > Multiple **integrations** (bidirectional)
- > **REST API** for automation
- > Events **enrichment** & **investigation**



Visualize

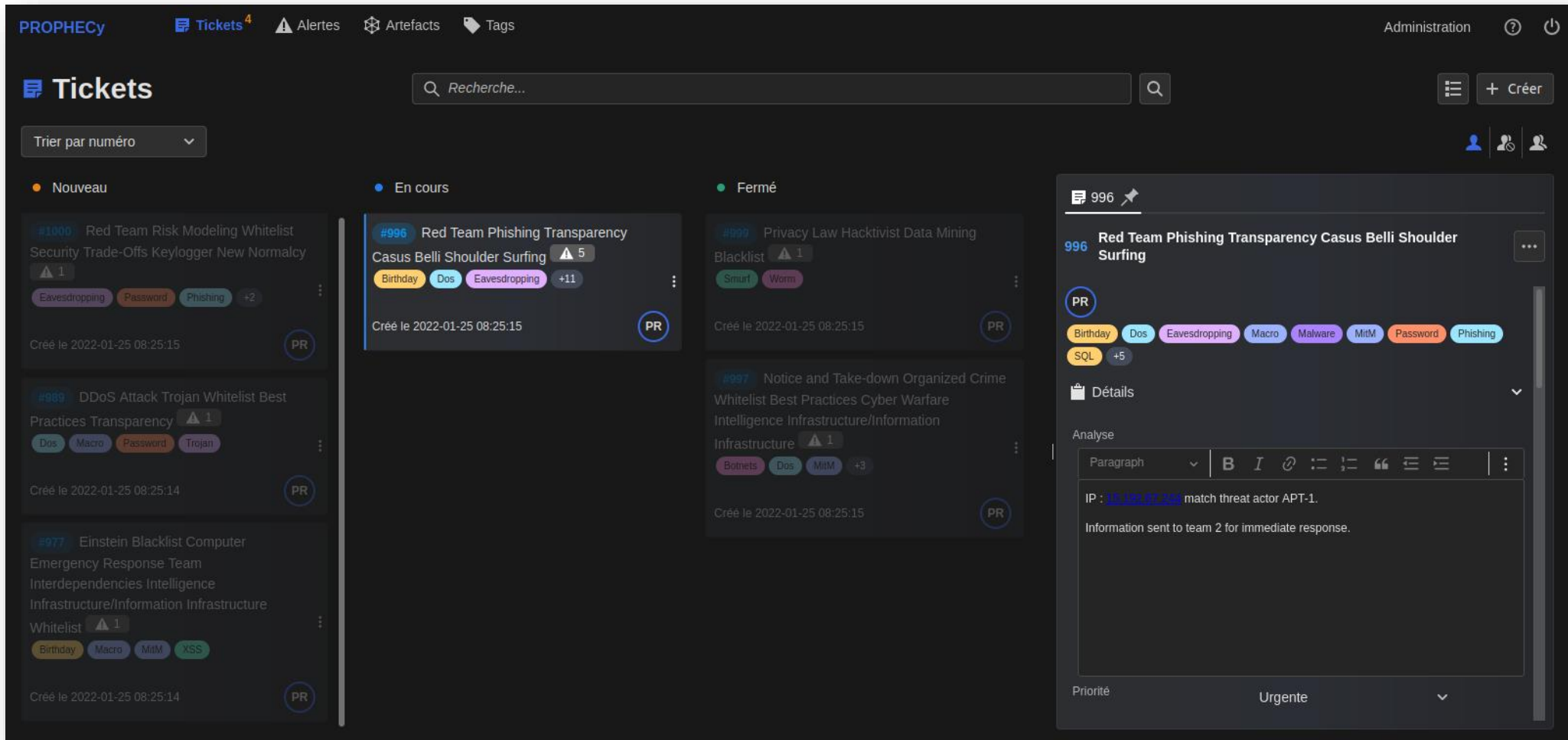
- > **Correlate** events automatically
- > **Materialize** links between events
- > **Contextualize** dynamically event



The screenshot displays the PROPHECy Alerts interface. The main view is a network graph showing relationships between alerts, artifacts, and tickets. The graph is centered on a red alert node labeled 'user:perez'. Other nodes include artifacts (blue) and tickets (yellow), all connected by orange lines. A sidebar on the left provides filters: 'Trier par date', 'Tout', and 'Tout'. A legend indicates 'Alerte racine' (red), 'Artefact' (blue), and 'Ticket' (yellow). A right-hand panel shows the details for 'user:perez', including tags like 'Birthday', 'Botnets', 'Dos', 'Eavesdropping', 'Macro', 'Malware', 'MitM', 'Password', and 'Phishing'. Below the tags is a 'Chronologie' bar chart showing alert frequency over time, and a list of 15 alerts, with the top ones being '235 Sneakernet Botnet', '41 Transparency Hacktivism', '293 Lawfare Malware Lawfare Whitelist', and '903 National Security State Affiliation Zero-Day Exploit Computer Network Attack'.

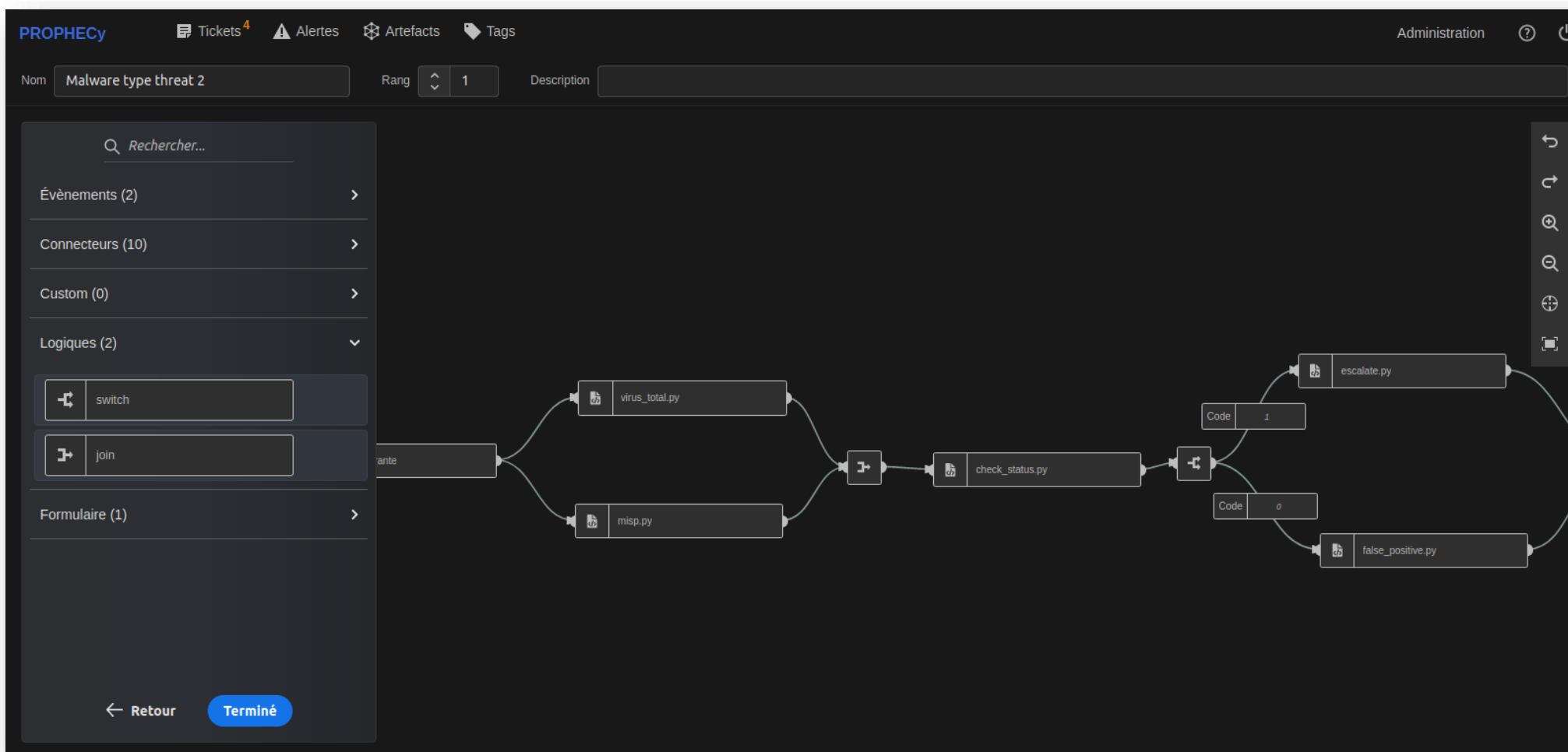
Understand

- > **Streamline** ticket handling and collaboration (Kanban)
- > **Prioritize** and categorize with tags
- > **Cross analyze** events through a modern UI



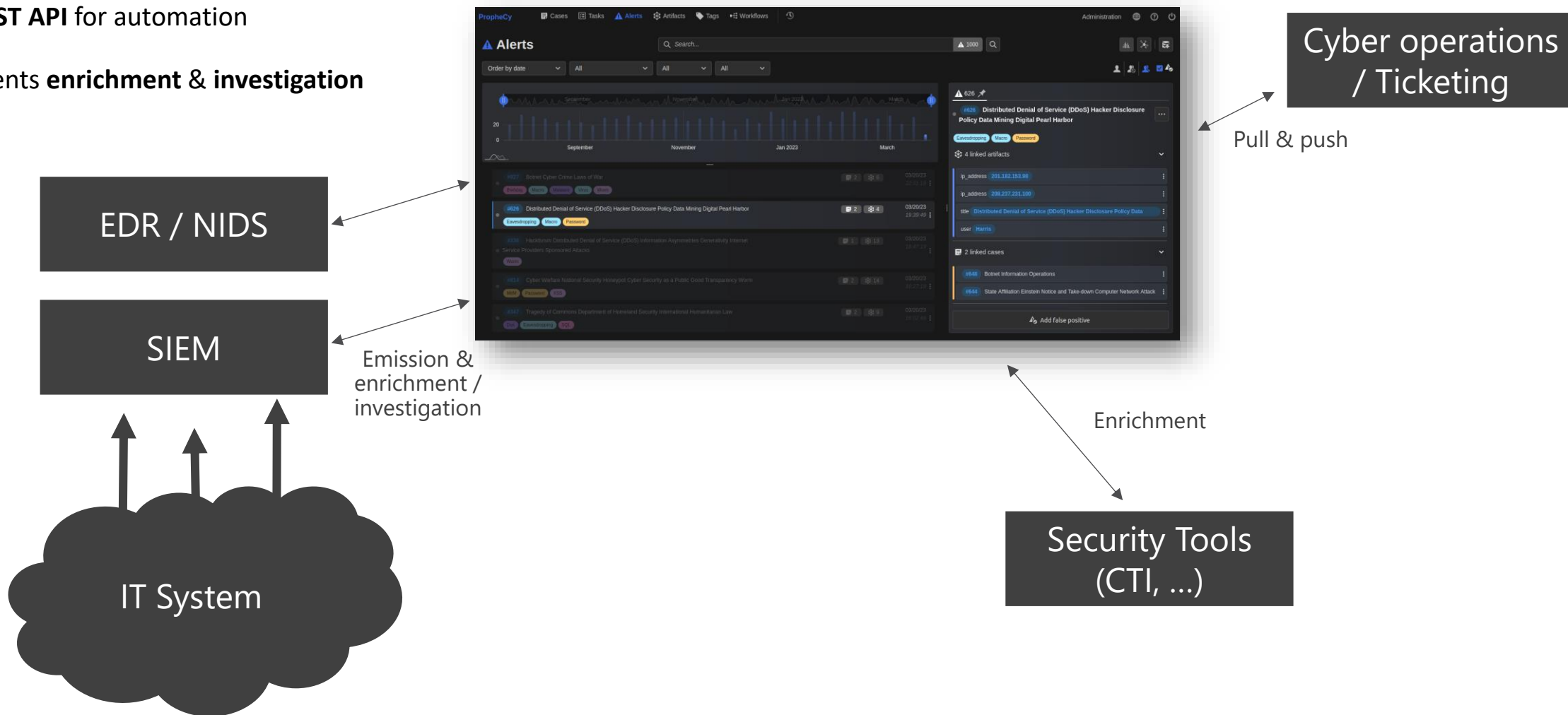
Automate

- > **Automate** each step of event analysis
- > **Orchestrate** with workflow
- > **Provide intelligence** out of the box : shared library of connectors and



PropheCy

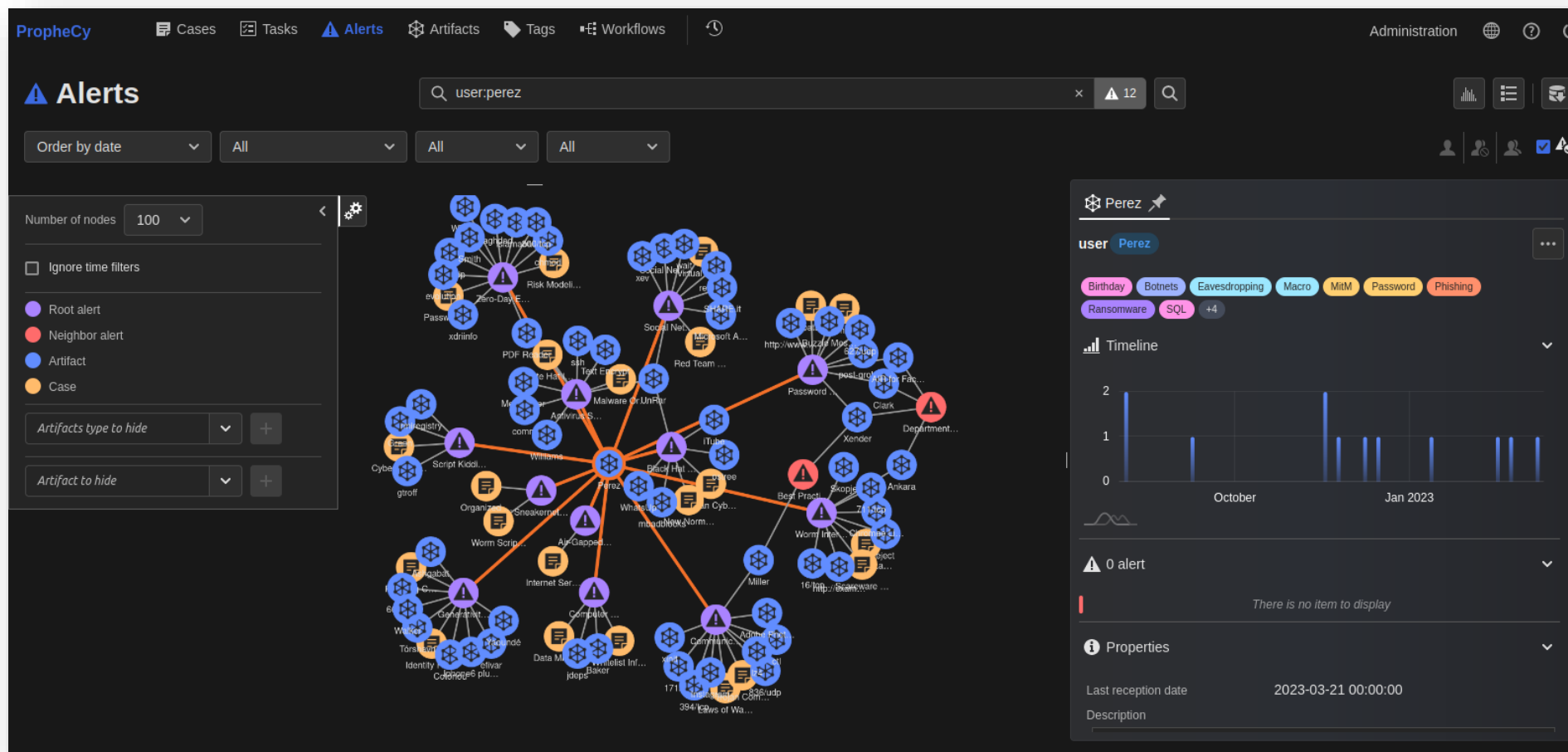
- > Multiple **integrations** (bidirectional)
- > **REST API** for automation
- > Events **enrichment & investigation**



PropheCy

Visualise

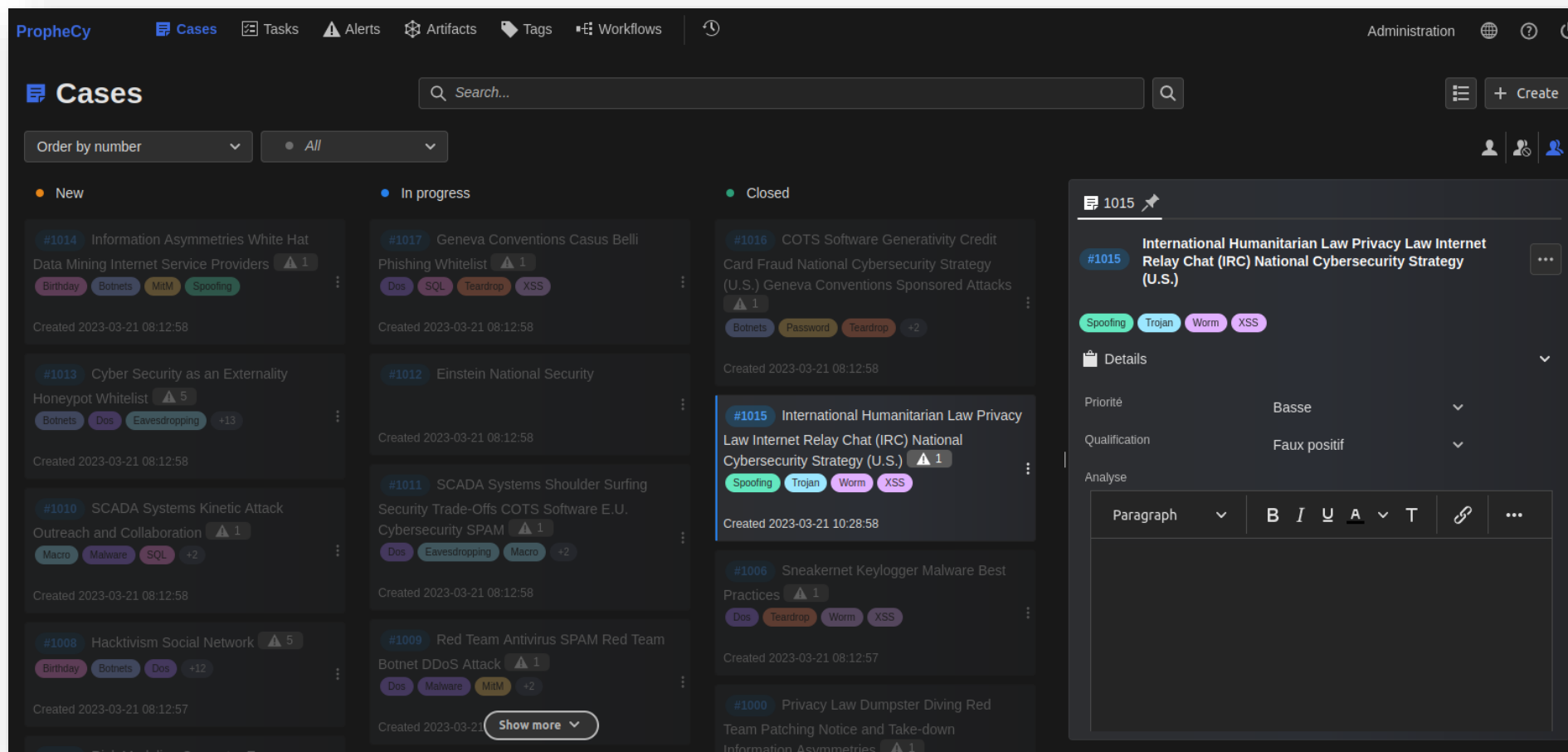
- > Automatically **correlate** security events
- > **Link** artifacts between similar events
- > Dynamic events **contextualisation**



PropheCy

Understand

- > Facilitate case handling & collaborative work (Kanban board)
- > Case **priorisation** (tags)
- > **Easy-to-use** & modern Web UI for in-depth event analysis



PropheCy

Automate

- > **Automate** investigations
- > Workflows **orchestration**
- > **Triggered automatically** or manually

