

SOLUTION BRIEF

DFLabs IncMan SOAR - Meeting the General Data Protection Regulation (GDPR).

This Solution Brief outlines how the organizations with
GDPR mandates can benefit from IncMan SOAR.

DFLABS.COM

Automate.
Orchestrate.
Measure.



DFLabs IncMan SOAR, the pioneering Security Orchestration, Automation and Response (SOAR) platform for SOCs, CSIRTs and MSSPs, enables organizations that must be compliant with GDPR to adhere to breach notification requirements by automating associated processes,

prioritizing incident response actions, and managing notification distribution and subsequent documentation for any incident.

This Solution Brief outlines how organizations with GDPR mandates can benefit from IncMan SOAR.

Executive Summary.

The EU General Data Protection Regulation (GDPR) was adopted in April 2016 and was formally enforced in May 2018.

The GDPR emphasizes transparency, security and accountability by data controllers. GDPR introduces mandatory Data Protection Impact Assessments (DPIA) for those organizations involved in high-risk processing, for example where a new technology is being deployed, where a profiling operation is likely to significantly affect individuals, or where there is large scale monitoring of a publicly accessible area.

A DPIA is the process of systematically considering the potential impact allowing organizations to identify potential privacy issues before they arise and come up with a way to mitigate them.

In addition, Data Processors must implement an internal breach notification process and must inform the supervisory authority of a breach within 72 hours, communicate the breach to affected data subjects without due delay or face a penalty of up to EUR 20,000.00 or 4% of worldwide annual turnover for the preceding financial year.

GDPR Requirements.

Data Processors must:

- Establish formalized incident response procedures
- Implement an internal breach notification process
- Communicate the personal data breach to the data subject without delay
- Notify supervisory authority within 72 hours
- Be compliant or face a fine of up to EUR 20,000.00 or up to 4% of annual turnover

Data Processors must implement an internal breach notification process.

Key Takeaways.

1. DFLabs IncMan SOAR provides capabilities to automate and prioritize incident response and related enrichment and containment tasks, distribute appropriate notifications and implement an incident response plan (IRP) in case of a potential data breach.
2. IncMan SOAR handles different stages of the incident response and breach notification process including providing advanced reporting capabilities with appropriate metrics and the ability to gather or share intelligence with third parties.

**Automate.
Orchestrate.
Measure.**

IncMan SOAR and GDPR Need in IR.

As the number of breaches has risen and cyber attacks have become more sophisticated, authorities have recognized a need for increased data protection regulation. The number of simultaneous processes required in a typical forensic or incident response scenario has also grown. Processes need to cover a broad spectrum of technologies and use cases, must be standardized and must perform clearly defined, fully documented actions based upon regulatory requirements, international standards and established best practices.

Additionally, context enrichment and threat analysis capabilities must be integrated to facilitate and automate data breach reporting and notification within the timeframe specified by GDPR.

Lastly, customized playbooks must be created to permit rapid response to specific incident types, aid in prioritizing tasks, assignment to individual stakeholders, and to formalize, enforce and measure specific workflows.

Having a platform in place to formalize and support these requirements is crucial. DFLabs IncMan SOAR provides all the necessary capabilities to facilitate this.

Not only do organizations need an incident response plan, but they must also have a repeatable and scalable process, as this is one of the steps towards compliance with the GDPR's accountability principle, requiring that organizations demonstrate the ways in which they comply with data protection principles when transacting business. They must also be able to ensure that they will meet the 72-hour breach notification requirement or face a stiff penalty.

DFLabs IncMan SOAR and fulfilling GDPR requirements:

- Demonstrating compliance
- Integrated GDPR incident response and breach notification playbooks
- Formalized, repeatable and enforceable IR workflows for GDPR
- Achieving breach notification within 72 hours and notifying third parties
- Context enrichment and threat analysis capabilities
- Gather intelligence from various sources and securely share Information with third parties
- Integrated KPIs and reporting

Organizations must establish a framework for accountability, as well as a culture of monitoring, reviewing and assessing their data processing procedures to detect, report and investigate any personal data breach.

IncMan SOAR implements granular and use-case specific incident response procedures with data segregation and critical security control requirements. To enable incident response and breach notification in complex organizations and working across different regions, IncMan SOAR can be deployed as a multitenant solution with granular role-based access.

Automated responses can be executed to save invaluable time and resources and reduce the window from discovery to containment for an incident.

Organizations can easily prepare advanced reports from automatically collected incident and forensic data, and distribute notifications based on granular rules to report a breach and notify

affected customers when required to comply with GDPR and avoid a financial penalty.

Finally, the ability to gather and share intelligence from various sources by anonymizing the data to share safely with third party protect the data without inhibiting the investigation. IncMan SOAR contains a Knowledge Base module to document playbooks, threat assessment, situational awareness and best practices which could be shared and transferred across the organization.

Speak to one of our representatives to find out more.

Organizations must establish a framework for accountability, as well as a culture of monitoring, reviewing and assessing.

Automate.
Orchestrate.
Measure.

| About Us.

DFLabs is an award-winning and recognized global leader in Security Orchestration, Automation and Response (SOAR) technology.

Its pioneering purpose-built platform, IncMan SOAR, is designed to manage, measure and orchestrate security operations tasks, including security incident qualification, triage and escalation, threat hunting and investigation, and threat containment.

IncMan SOAR harnesses machine learning and automation capabilities to augment human analysts to maximize the effectiveness and efficiency of security operations teams, reducing the time from breach discovery to resolution and

increasing the return on investment for existing security technologies.

As its flagship product, IncMan SOAR has been adopted by Fortune 500 and Global 2000 organizations worldwide.

The company's management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121.

DFLabs has operations in Europe, North America and EMEA.

For more information, visit our website www.dflabs.com or connect with us on Twitter [@DFLabs](https://twitter.com/DFLabs).



CONTACT US:

BOSTON - UNITED STATES

150 State Street
Boston, 02109

T – +1 201 579 0893

E – sales@dflabs.com

LONDON - UNITED KINGDOM

1 Primrose Street
London, EC2A 2EX

T – +44 203 286 4193

E – sales@dflabs.com

MILAN - ITALY

Via Bergognone, 31
20144, Milan

T – +39 0373 82416

E – sales@dflabs.com

CUSTOMER SUPPORT:

T – +39 0373 82416

E – support@dflabs.com

Automate.
Orchestrate.
Measure.

DFLABS.COM