SOLUTION BRIEF

DFLabs' IncMan DFIR - Digital Forensics and Incident Response Platform.

This Solution Brief outlines how your organization can benefit from IncMan DFIR.

DFLABS.COM

Automate.
Orchestrate.
Measure.

DFLABS
CYBER INCIDENTS UNDER CONTROL

DFLabs' IncMan DFIR provides cyber security teams with capabilities to define the roles and responsibilities of Incident Response Stakeholders, to characterize incidents, and the relationships to policies and procedures and reporting requirements.

This Solution Brief outlines how your organization can benefit from IncMan DFIR.

IncMan DFIR works best for smaller Digital Forensics and Incident Response teams of around 1 to 5 analysts.

IncMan DFIR utilizes Semi-Automated Check List Playbooks that allow SOC teams to orchestrate actions and daemons without creating workflows.

IncMan SOAR vs. IncMan DFIR: What's the Difference?

To understand why IncMan DFIR is the right solution for your organization, you need to learn how IncMan DFIR distinguishes itself from IncMan SOAR as a highly targeted SOAR solution.

Unlike IncMan SOAR, which is recommended for structured SOC and Incident Response teams consisting of a minimum of 5 analysts, IncMan DFIR works best for smaller Digital Forensics and Incident Response teams of around 1 to 5 analysts.

Furthermore, what makes IncMan DFIR special is the fact that you can manage all DFIR tools in an all-in-one platform which supports Digital Forensics with the goal of reducing human error and improving the incident response time.

IncMan DFIR utilizes Semi-Automated Check List Playbooks that allow SOC teams to orchestrate actions and daemons without creating workflows. Also, via Lab Management, organizations can have access to a complete forensic laboratory and track different devices, software, and tools.

For Small Digital Forensics and Incident Response Teams.

Improvements to an incident response team's toolsets and procedures can have a big impact on their incident response time. Metrics that track the amount of time needed to verify that the resolution of the incident was completed, can improve the organization's overall work environment.

As attacks have become more sophisticated, the need for Incident Response Teams has grown. The number of simultaneous processes required in a typical forensic or incident response and evidence collection scenario is constantly growing. Such processes need to be standardized and must perform clearly defined actions based upon international standards and established best practices while being fully documented.

DFLabs' IncMan DFIR offers a digital forensics and incident response platform designed for managing, storing and reporting information gathered during digital investigative operations with the option for segregation of duties, incident categorization, a knowledge base module for defining policies and procedures, advanced reporting and integrations with common forensic tools to support investigators in performing incident, evidence, and records management.

DFLabs' IncMan DFIR offers a digital forensics and incident response platform designed for managing, storing and reporting information gathered during digital investigative operations

Once an incident is created in IncMan DFIR, an automated response to update and prioritize different tasks can be activated and assigned to the appropriate team.

It is possible to ingest feeds from various 3rd party technologies such as SIEM events, email from ticketing systems, Forensic Tools, data from malware analyzers and from all devices that can send syslog messages. Alerts are collected and escalated to be converted into incidents.

There is also an option of using web forms that can be made available via web portal or intranet to enable users to report incidents to the Security Operation Center (SOC) or Cyber Security Incident Response Team to initiate investigations. Once an incident is created in IncMan DFIR, an automated response to update and prioritize different tasks can be activated and assigned to the appropriate team. Finally, IncMan DFIR is integrated bi-Directionally with DFLabs IncMan SOAR and any third party via API Connector.

The overall benefit is that the IncMan DFIR can assess the potential damage and risk to provide an effective and efficient response and conduct a forensic investigation.

How DFIR Teams Can Benefit From DFLabs' IncMan.

There are multiple ways that an organization can leverage DFLabs' IncMan DFIR in the incident response life cycle to orchestrate processes and duties as well as to support forensic activities.

One way to use IncMan DFIR is as the centralized incident response management platform in the SOC environment supporting multiple 3rd party technologies, immediately gaining the benefit of the core platform capabilities such as repeatable and measurable workflows, a dedicated knowledge base, and comprehensive incident reporting.

Another way in which IncMan DFIR can be used as a powerful case management platform with integrated forensics capabilities is through automatic upload of acquisition data from supported forensic tools, such as FTK, EnCase, Xways, Tableau and ICS Solo, uploading of snapshots and bookmarks, automated email integration, forensic lab dedicated to managing forensic images as well as highly flexible and customizable action templates out of the box.

DFLabs' IncMan DFIR can also centrally manage dedicated instances of IncMan on a per client basis, providing data segregation, dedicated playbooks and knowledge base to individual clients.

DFLabs for DFIR at a Glance.

IncMan DFIR supports investigators in performing incident management, evidence and records management, providing a platform for preparing notes, managing forensic images with automatic upload of acquisition data, snapshots and bookmarks as well as generating chain of custody reports.

IncMan DFIR imports data from all leading forensic tools, such as FTK, EnCase, Xways, Tableau and ICS Solo.

The table below highlights some of the benefits that IncMan DFIR offers to Computer Security Incident Response Teams in order to manage, store and report on information gathered during digital investigative operations across the entire incident life cycle.

IncMan DFIR supports investigators in performing incident management, evidence and records management, providing a platform for preparing notes, managing forensic images with automatic upload of acquisition data, snapshots and bookmarks as well as generating chain of custody reports.

IncMan DFIR vs. IncMan SOAR

IncMan Features	DFIR	SOAR	MSSP
SOAR Playbooks	✗	✓	✓
Check List Playbooks	✓	✓	✓
TRIAGE	✗	✓	✓
High Availability and Cluster	✗	✓	✓
Home for Analysts	✗	✓	✓
Watcher Groups	✗	✓	✓
Entities	✗	✓	✓
Advanced Incident Search Bar	✗	✓	✓
Automated Responder Knowledge (ARK)	✗	✓	✓
Syslog Event Automation	✗	✓	✓
Forensic Lab Management	✓	✗	✗

Speak to one of our representatives to find out more.

Automate.
Orchestrate.
Measure.

About Us.

DFLabs is an award-winning and recognized global leader in security orchestration, automation, and response (SOAR) technology. 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. Its flagship product, IncMan SOAR, is multi-patented, and it has been adopted by Fortune 500 and Global 2000 organizations worldwide. DFLabs has operations in EMEA Americas and APAC. For more information, visit www.dflabs.com.

DFLABS.COM

DFLABS
CYBER INCIDENTS UNDER CONTROL

HEAD OFFICE

DFLabs S.p.A
Address: Via Pietro Donati,
16 26013 Crema (CR)
T - +39 (0) 373-82416
E - info@dflabs.com

SALES

ITALY
Via Bergognone, 31
20144, Milan
T - +1 201 579 0893

UNITED KINGDOM
1 Primrose Street
London, EC2A 2E
T - +44 203 286 4193

UNITED STATES
200 Portland Street
Boston, 02114
E - sales@dflabs.com

CUSTOMER SUPPORT

T - +39 0373 82416
E - support@dflabs.com

Automate.
Orchestrate.
Measure.