SOLUTION BRIEF

DFLabs IncMan SOAR - The Managed Detection and Response Delivery Platform for MSSPs and MDRs.

This Solution Brief outlines how MSSPs and MDRs can benefit from and monetize IncMan SOAR.

DFLABS.COM

Automate.
Orchestrate.
Measure.

DFLABS
CYBER INCIDENTS UNDER CONTROL

DFLabs IncMan SOAR increases MSSPs economies of scale and enables the delivery of premium and advanced security services.

This Solution Brief outlines how MSSPs and MDRs can benefit from and monetize IncMan SOAR.

Executive Summary.

The worldwide MSSP market is projected to grow at 15-20% year on year according to Gartner[1], with Managed Detect and Response services predicted to be used by 15% of midsized and large enterprises by 2020[2]. This growth is driven by a growing skills shortage, an escalating threat environment and the increasing sophistication of the threats themselves

Many organizations are struggling to hire and retain sufficient security resources with the required breadth of skills to deal with all cyber security tasks.

At the same time, the number of providers offering managed security services has also ballooned, with large IT service providers, Telcos and even vendors offering services around their own portfolio.

Managed Security Service Providers must evolve to become Managed Detect and Response providers, and must leverage greater economies of scale while delivering more advanced services than their growing pool of competitors to differentiate themselves.

IncMan SOAR – The Ultimate Delivery Platform for MSSPs and MDRs.

There has been a gap in the availability of purpose-built platforms designed for MSSPs to deliver security monitoring and incident response services. Many providers have opted to build their own backend and platform, with mixed results. Others have repurposed adjacent technologies such as Security Incident and Event Management or Ticket Management solutions, but have had to improvise around the shortcomings of using a technology not directly conceived of for their use case.

DFLabs IncMan SOAR for MSSPs is a purpose-built platform designed for MSSPs to deliver security monitoring and incident response services.

- Innovative pay as you grow licensing model
- Integrated support for Multi Tenancy, High Availability and Load Balancing
- Scalable architecture that can be hosted on Cloud Service Providers or integrated with NAS and SANs
- Tailor made platform to provide advanced and premium MSSP services
- Custom script execution and bidirectional SOAP API for easy MSP backend integration

At the heart of IncMan SOAR is the R^3 Rapid Response Runbook engine. R^3 Runbooks are created using a visual editor and support granular, stateful and conditional workflows to orchestrate and automate incident response activities such as incident triage, stakeholder notification, data and context enrichment and threat containment. R^3 Runbooks are supported by capabilities to empower incident responders in assessing, investigating and hunting for threats, and to gather, maintain and transfer knowledge within IR and SOC teams.

R^3 Runbooks can be created and assigned to individual customers, multiple per customer in fact, to capture, enforce and measure customer specific workflows.

DFLabs patent pending Automated Responder Knowledge (ARK) module applies machine learning to historical responses to incidents and recommends relevant playbooks and paths of action to manage and mitigate threats across customers and tenants. Put simply:

- It is possible to manage more incidents for more customers with fewer security analysts
- The ceiling for diminishing returns in scaling up a SOC is raised
- The economies of scale in running a SOC are increased

Data Processors must implement an internal breach notification process.

Automate.
Orchestrate.
Measure.

IncMan SOAR for MSSPs at a Glance.

IncMan SOAR is the pioneering Security Automation and Orchestration platform to manage, measure and orchestrate security operations tasks including security incident qualification, triage and escalation, threat hunting & investigation and threat containment. IncMan SOAR harnesses machine learning and automation capabilities to augment human analysts to maximize the effectiveness and efficiency of SOCs and CSIRTs, reducing the time from breach discovery to resolution.

The table below highlights some of the benefits that IncMan SOAR offers to Managed Security Service Providers who offer security monitoring, incident response and advanced threat management services:

Core MSSP Benefits	IncMan SOAR Solution
Increase economies of scale, reduce the cost per handled incident	Customizable playbooks and runbooks that automate many manual actions, keeping humans "In the loop" and "on the loop"
Eliminate manually writing and maintaining customer playbooks and incident response procedures	Create a library of dedicated, customizable and granular playbooks for every individual customer
Establish a knowledge base to disseminate, share and transfer knowledge from experienced to novice analysts and across the team, or for specific verticals or regions	IncMan SOAR contains a knowledge base module to document playbooks, threat assessment, situational awareness and best practices Segregated and dedicated knowledge bases can be assigned to individual or groups of customers
Offer a dedicated virtual SOC for customers with data segregation or critical security requirements	Deploy as a multi-tenant solution with granular role-based access. Business units and clients can have their own dedicated virtual CSIRT
Offer remote containment of threats	IncMan SOAR provides a centralized repository to handle and store artifacts related to various incidents
Gain automated responder knowledge	Integration with forensic duplicators, eDiscovery management, evidence management in a dedicated forensic laboratory and an extensive inventory of all forensics capabilities

Additional Benefits Include:

- Highly flexible and customizable, with over 100 playbook templates included out of the box
- Support for hundreds of 3rd party technologies via Syslog, CEF and Email, and over 45 bidirectional connectors
- A correlation engine that correlates all relevant IOCs and artifacts between incidents
- Multi-tenancy and granular role-based access
- Customizable and granular playbooks
- Threat intelligence fusion and sharing
- Powerful case management with integrated forensics capabilities
- Automate and orchestrate MSSP SOC processes and duties
- Effort cost per incident and per customer is reduced
- Premium services can be added right out of the box
- Shared platform and a single pane of glass to deliver standard and premium managed security and MDR services
- Automatically correlates and re-applies playbooks across Tenants in multi-user and MSSP environments

Automate.
Orchestrate.
Measure.

How MSSPs Can Monetize IncMan SOAR.

There are multiple ways that an MSSP can leverage DFLabs IncMan SOAR to reduce costs and to offer premium security services and capabilities. The easiest way is to use IncMan SOAR as the centralized incident response management platform in the MSSPs SOC and immediately gain the benefit of the core platform capabilities such as granular and customizable playbooks, the automation of workflow tasks, a dedicated knowledge base and comprehensive incident reporting.

In addition, individual IncMan SOAR capabilities can be sold as a premium service, for example a remote containment service based on remotely executing automated containment responses such as disabling a user in Active Directory or blocking a specific connection on a firewall.

The platform can also centrally manage dedicated instances of IncMan SOAR on a per customer basis, providing data segregation, dedicated playbooks and runbooks and knowledge base to provide a virtual SOC service.

IncMan SOAR MSSP Delivery Models.

Intelligence-drive MSSP Platform	Premium MSS Services	Virtual SOC	Managed Detection and Response
• IncMan SOAR is used as the primary platform to deliver a shared service • Granular and customizable playbooks for individual customers • Automation of common incident response workflows • Shared knowledge base	• IncMan SOAR is used as the primary platform to deliver a shared service • Premium services are offered based on the IncMan SOAR platform • Remote threat containment • Dedicated knowledge base • Custom runbooks	• IncMan SOAR is used as the primary platform to deliver a multitenant service • Customers receive a managed, hosted and dedicated instance of IncMan SOAR • The MSSP can centrally manage all customer instances	• Advanced threat defense based on tailored detection stack • IncMan SOAR is deployed as the primary platform to deliver a multitenant service • DFLabs's Automated Responder, Knowledge (ARK), runbooks and ther advanced capabilities are fully leveraged to deliver MDR services

Innovative MSSP Licensing.

DFLabs has a pay as you grow licensing model that is designed to enable MSSPs to deliver competitive premium and advanced security services, and to increase their economies of scale to manage more incidents for more customers at a lower overall cost.

Speak to one of our MSSP Channel 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.

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 & 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.

DFLABS.COM

DFLABS
CYBER INCIDENTS UNDER CONTROL

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.