SOLUTION BRIEF

DFLabs IncMan SOAR - The Security Orchestration, Automation and Response Platform for SOCs.

This Solution Brief outlines how DFLabs IncMan SOAR is designed to automate, orchestrate and measure security operations and incident response processes and tasks to improve the overall effectiveness and efficiency of your SOC.

DFLABS.COM

Automate.
Orchestrate.
Measure.

DFLABS
CYBER INCIDENTS UNDER CONTROL

DFLabs IncMan SOAR, the award-winning and pioneering Security Orchestration, Automation and Response (SOAR) platform for Security Operations Centers (SOCs) is a purpose built platform designed to manage security operations.

This Solution Brief outlines how DFLabs IncMan SOAR enables you to automate, orchestrate and measure security operations and incident response processes and tasks to improve the overall effectiveness and efficiency of your SOC.

Minimize Resolution Time By 90%

Maximize Analyst Efficiency By 80%

Increase Handled Incidents By 300%

Executive Summary.

DFLabs IncMan SOAR provides a library of customizable playbooks for different threat and incident response scenarios such as malware, data loss or regulatory breach notification. The solution further provides capabilities to support incident responders in assessing, investigating and hunting for threats, and to gather, maintain and transfer knowledge within the secuirty operations center team.

DFLabs IncMan SOAR acts as a force multiplier making it possible to manage more incidents in less time with fewer security analysts, and to do so in a repeatable, measurable and enforceable manner.

At the heart of IncMan SOAR is our 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 activites such as incident triage, stakeholder notification, data context and enrichment and threat containment. R^3 Runbooks are enhanced by capabilities to empower incident responders by assessing, investigating and hunting for threats, and to gather, maintain and transfer knowledge between IR and SOC teams.

Our patent-pending Automated Responder Knowledge (ARK) module applies machine learning to historical responses to threats and recommends relevant runbooks and paths of action to manage and mitigate them.

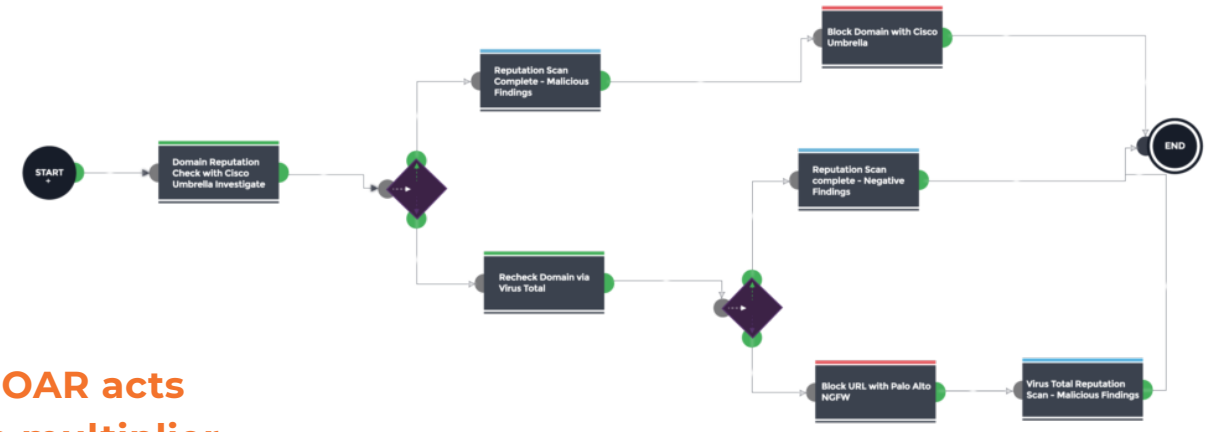

Figure 1. R^3 Rapid Response Runbook Example.

IncMan SOAR acts as a force multiplier, enabling SOCs to do more with less.

Automate.
Orchestrate.
Measure.

Features.

DFLabs IncMan SOAR provides orchestration and automation features to automate, orchestrate and measure incident response processes. The solution can ingest the data of hundreds of third party security technologies with many certified bidirectionl integrations, including Cisco ThreatGrid and Umbrella, IBM QRadar, Splunk, McAfee, Palo Alto and many others.

IncMan SOAR has been designed with industry standards, regulatory frameworks and best practices in mind, suporting ISO, GDPR, NIST and SEC regulations amongst others.

Automation.

R^3 Rapid Response Runbooks

- Support the creation of customizable automation runbooks
- Complex stateful and conditional logical decision making to pursue a variety of alternative responses
- Over 100 out of the box automation actions
- Graphical visual editor

Full Incident Lifecycle Automation

- Triage and notification
- Context enrichment
- Hunting and investigating
- Threat containment

Dual-Mode Actions

- Combine manual, semi-automated and automated actions
- Automate the action without automation the decision

Automated Responder Knowledge

- Learns from historial incidents and your team's responses to them
- Advise analysts about similar or related incidents and suggest relevant and related playbooks
- Speeds up response times and facilitates knowledge sharing

Orchestration.

Aggregation and Correlation of Security and Incident Data

- Support for hundreds of third party security technologies via Syslog, CEF and Email parsing
- Over 45 bidirectional connectors
- Database querying
- Custom script execution
- Bidirectional SOAR API

Customizable, Linear and Conditional Playbooks

- Over 100 customizable playbooks for individual incident types or threats and regulatory frameworks
- Automatically correlates and reapplies playbooks across tenants in multi-user and MSSP environments
- Professional services are available to assist in customization

Integrated Knowledgebase Module

- Share playbooks, threat intelligence, situational awareness and best practices to facilitate knowledge transfer and continuity
- Library includes GDPR, ISO, NIST and other regulatory frameworks

Powerful Case Management

- Integrated forensics capabilities
- Forensics, response system analysis and evidence management
- Collaboration with diverse stakeholders
- Secure collaborative platform for data sharing and reporting

Automate.
Orchestrate.
Measure.

Analytics and Reporting.

Customizable Dashboards and Widgets

- Support for a huge variety of key performance indicators and metrics
- Visualize data with charts, graphs, tables and meters

Integrated Reporting Engine with Templates for:

- Operational performance
- Incidents
- Threats
- Regulatory compliance
- Over 140 customizable KPI and reporting templates

Full Incident Phase Management

- Measure every individual phase of the IR workflow
- Optimization, benchmarking and SLA calculation

Threat and Incident Data Visualization and Analysis

- Analysis and visualization of indicators of compromise and incident observables
- Automated threat intelligence fusion
- Support for STIX, TAXII, OpenIOC, MISP and many open source commercial TI feeds

Deployment.

IncMan SOAR can be deployed as a virtual machine and/or decidated HW appliance

- High availability and load balancing
- Multitenant architecture
- Scalable platform can be integrated with NAS and SAN

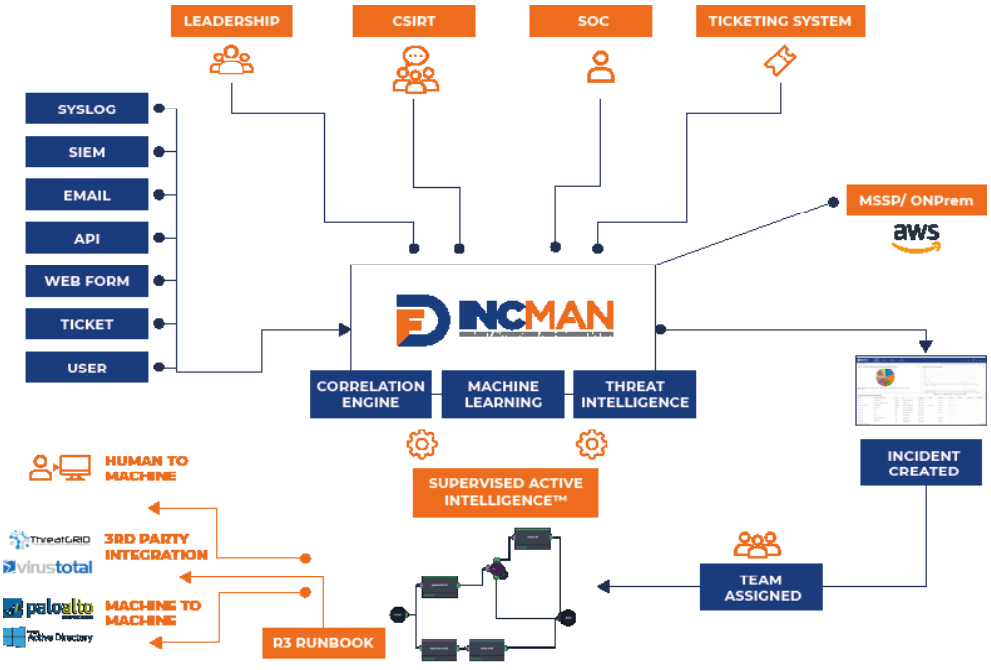

Figure 2. IncMan SOAR Deployment Overview.

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.