SOLUTION BRIEF

DFLabs IncMan SOAR - The Digital Forensic Evidence and Case Management Platform for CSIRTs.

This Solution Brief outlines how IncMan SOAR can benefit CSIRTs.

DFLABS.COM

Automate.
Orchestrate.
Measure.

DFLABS
CYBER INCIDENTS UNDER CONTROL

DFLabs IncMan SOAR provides a Computer Security Incident Response Team (CSIRT) 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 the CSIRT teams can benefit from IncMan SOAR.

Executive Summary.

The CSIRT within an organization is a centralized function for information security incident management as well as response. CSIRTs can come in all shapes and sizes and serve diverse constituencies.

The aim of a CSIRT is based on the business objectives of its constituent or parent organization, since protecting the critical assets is the key to success of both an organization and its CSIRT.

The ultimate goal of a CSIRT is to minimize and control the damage resulting from an incident, which is why so many different functions can be involved in some capacity.

Security Incident and Digital Evidence Management – The Ultimate Delivery Platform

As attacks have become more sophisticated, the need for Computer Security Incident Response Teams (CSIRTs) has grown.

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

As attacks have become more sophisticated, the need for Computer Security Incident Response Teams (CSIRTs) 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.

IncMan SOAR offers a digital forensic evidence management platform designed for managing, storing and reporting on 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.

It is possible to ingest feeds from various 3rd party technologies such as SIEM events, email from ticketing systems and 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 SOAR, an automated response to update and prioritize different tasks can be activated and assigned to the appropriate team.

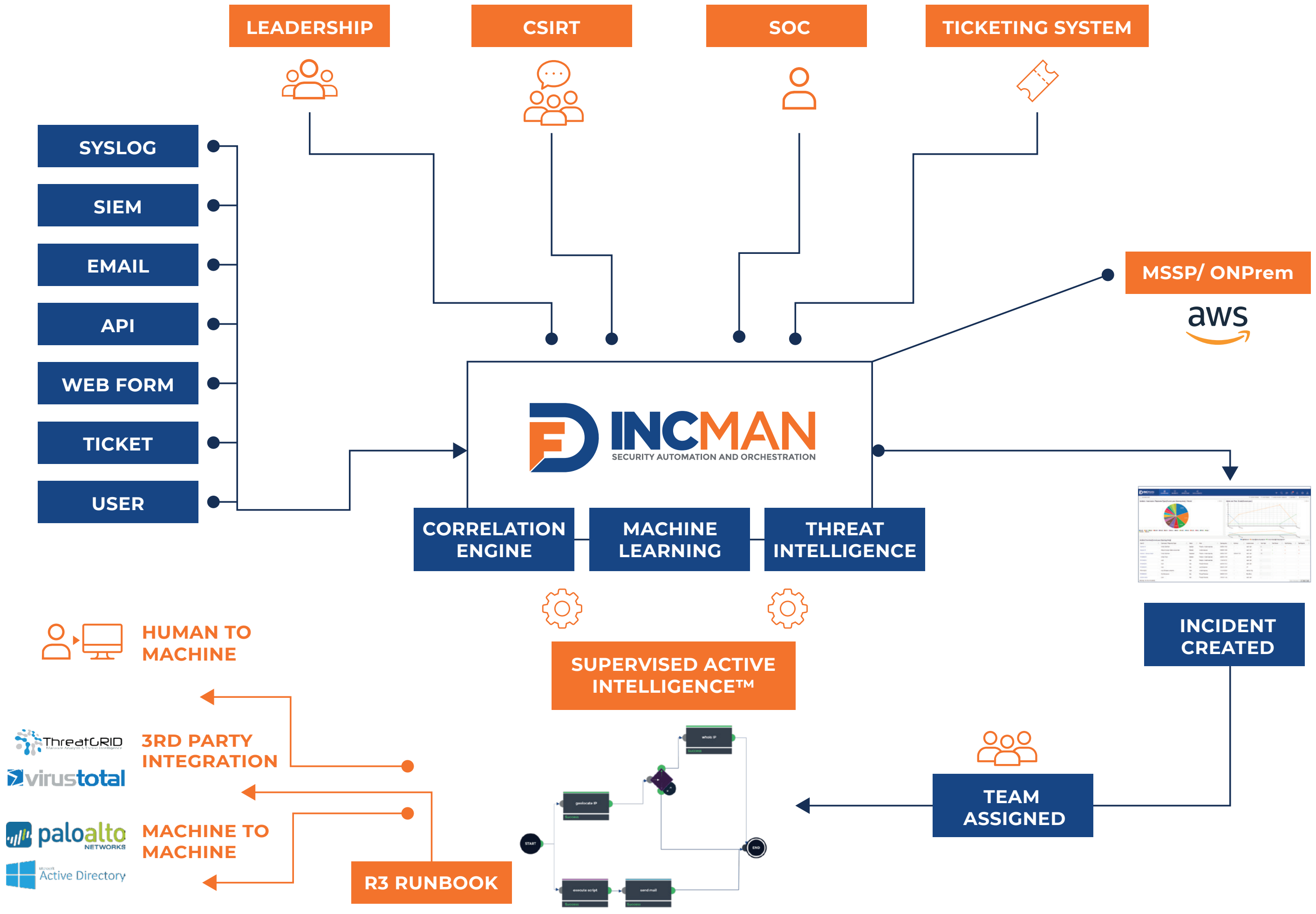

Figure 1. IncMan SOAR CSIRT Orchestration Model.

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

DFLabs for CSIRTs at a Glance.

IncMan SOAR for CSIRTs 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 SOAR 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 SOAR 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 lifecycle.

IncMan SOAR for CSIRTs supports investigators in performing incident management, evidence and records management.

Automate.
Orchestrate.
Measure.

IncMan SOAR for CSIRTs Benefits

Core CSIRT Benefits	IncMan SOAR Solution
Security assessment and cost analysis	Assess costs, financial impact and time spent associated with an incident, including the technical and non-technical repercussion
Eliminate manually writing and maintaining customer playbooks and incident response procedures	Create a library of dedicated, customizable and granular playbooks for every individual customer
Incident response case management with data segregation and role-based access	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
Artifact handling	IncMan SOAR provides a centralized repository to handle and store artifacts related to various incidents
Metrics, advanced reporting and correlation engine	Integration with forensic duplicators, eDiscovery management, evidence management in a dedicated forensic laboratory and an extensive inventory of all forensics capabilities
Evidence tracking and standardized labels proposed by the system	Chain of custody reporting for easy tracking of evidence including barcode labeling as well as CSIRTs standardized including dent/host/evidence/ clone labels with automated label suggestions
Fully customizable dashboards and widgets	Generate key metrics and customized KPI reports for supervisors and managers including a correlation engine that correlates all relevant IOCs and artifacts between incidents. IncMan SOAR also includes a correlation engine that correlates all relevant IOCs and artifacts between incidents.
Integrated knowledge base module	IncMan SOAR includes a knowledge base module to document playbooks, threat assessment, situational awareness and to transfer best practices from experienced to novice analysts and share knowledge across the CSIRT.

Automate.
Orchestrate.
Measure.

How CSIRTs Can Benefit from IncMan SOAR.

There are multiple ways that a CSIRT can leverage IncMan SOAR in the incident response lifecycle to orchestrate CSIRTs processes and duties, as well as to support forensic activities.

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

Another way in which IncMan SOAR can be used by CSIRTs can be as a powerful case management platform with integrated forensics capabilities including but not limited to 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.

The platform can also centrally manage dedicated instances of IncMan SOAR on a per client basis, providing data segregation, dedicated playbooks and runbooks and knowledge base to individual clients.

Speak to one of our representatives to find out more.

A CSIRT can leverage IncMan SOAR in the incident response lifecycle to orchestrate CSIRTs processes and duties, as well as support forensic acivities.

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
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.

DFLABS.COM