Recorded Future | DFLABS CYBER INCIDENTS UNDER CONTROL

JOINT SOLUTIONS

# DFLabs and Recorded Future: Simplifying Intelligence Gathering

## Combining Industry-Leading Threat Intelligence From Recorded Future With Automation and Orchestration Excellence From DFlabs

More than a third of security incidents take weeks to detect and even months to remediate.

### Solution Overview

DFLabs integration with Recorded Future enables automated information gathering from one of the industry's leading intelligence solutions to provide investigators with crucial details and context surrounding a potential incident.

By automating the information-gathering stage investigators will be able to better use their time investigating an incident rather than focusing this valuable time performing manual information gathering and the data correlation necessary to prioritize an event.

### The Problem

Cybersecurity attacks continue to evolve, and the security community has taken great strides to provide investigators with valuable information about their adversaries.

However, this valuable information is oftentimes scattered across many tools with varying degrees of confidence. This leaves investigators without a full understanding of the risk posed to their organization, which prevents confident decision-making at the most critical time in an investigation.

### The DFLabs and Recorded Future Solution

According to recent research conducted by Recorded Future, more than a third of security incidents take weeks to detect and even months to remediate. The majority of the cost associated with a breach can be drastically reduced by improving the speed and efficiency with which an organization responds to a threat.

DFLabs's partnership with Recorded Future combines this industry-leading threat intelligence data with the orchestration and automation capability necessary to quickly identify and remediate potential incidents before they can become a breach.

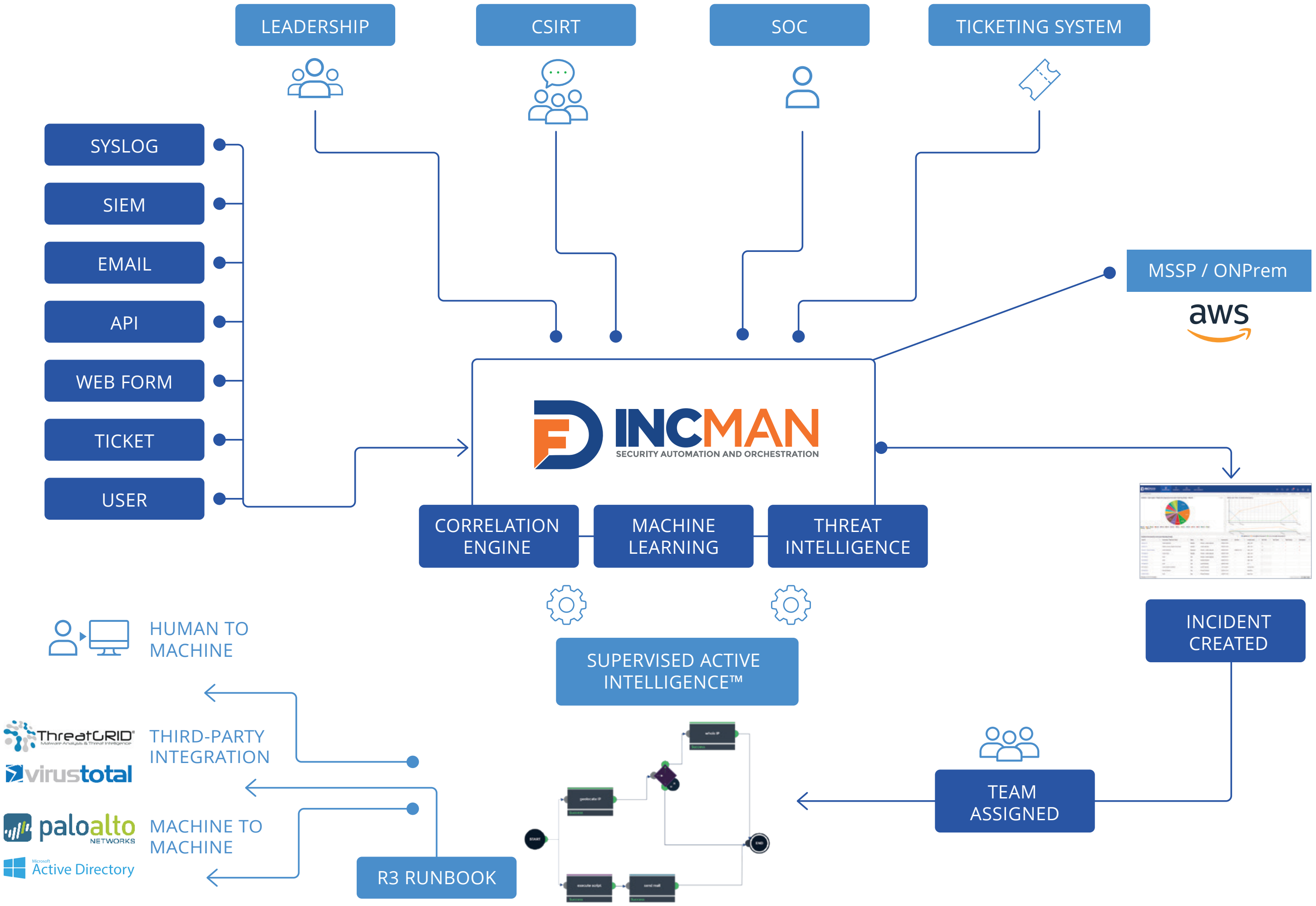
## DFLabs IncMan SOAR and Recorded Future solve these specific challenges:

- What intelligence data should I use and how can I use it?
- How can I cut down the time necessary for a proper investigation?
- Where should my intelligence data be best used?

## Combining IncMan SOAR, Recorded Future, and other security products enables enterprises to:

- Reduce incident resolution time by 90 percent
- Maximize security analyst efficiency by 80 percent
- Increase the number of handled incidents by 300 percent

## DFLabs IncMan SOAR Overview



### Challenges

- What intelligence data should I use and how can I use it?
- How can I cut down the time necessary for a proper investigation?
- Where should my intelligence data be best used?

### DFLabs And Recorded Future Solution

- Automate intelligence gathering to enrich data feeds
- Reduce investigator's mean time to respond by automating time-consuming investigation tasks
- Orchestrate additional technologies to respond faster to potential incidents

### Results

- Reduce incident resolution time by 90 percent
- Maximize security analyst efficiency by 80 percent

## About Recorded Future

Recorded Future is an industry-leading threat intelligence platform that aims to empower its customers with contextualized threat intelligence in real time, enabling organizations to proactively defend against threats at the speed and scale of the internet.

With billions of indexed facts, and more added every day, Recorded Future's Threat Intelligence Machine makes use of machine learning and natural language processing (NLP), to continuously analyze threat data from a massive range of sources to deliver contextualized intelligence to organizations in real time.

## About DFLabs IncMan SOAR

DFLabs IncMan Security Orchestration, Automation and Response (SOAR) platform improves security operations and incident response tasks, including threat validation, triage and escalation, context enrichment and threat containment.

IncMan SOAR uses machine learning and Rapid Response Runbooks (R3 Runbooks) as a force multiplier that has enabled security teams to reduce average incident resolution times by 90 percent and increase incident handling by 300 percent.

## Use Case

A WAF alert for a suspicious redirect is received and automatically triggers a new incident inside of IncMan SOAR. Using IncMan's integration with Recorded Future, the R3 Runbook begins to gather all the important information surrounding the redirected traffic. The domain reputation is checked against Recorded Future's extensive threat database while also being evaluated against its threat intelligence search capability. This capability allows for the domain to be simultaneously checked across multiple threat intelligence platforms such as STIX and MISP.

While the domain is being evaluated, the R3 Runbook also issues an IP reputation check to gather further information on our suspicious actor. Once all three of these reputation checks have been completed, the R3 Runbook encounters its first conditional action where the results of the information gathered can be evaluated together, providing a broader picture of the malicious nature of this communication.

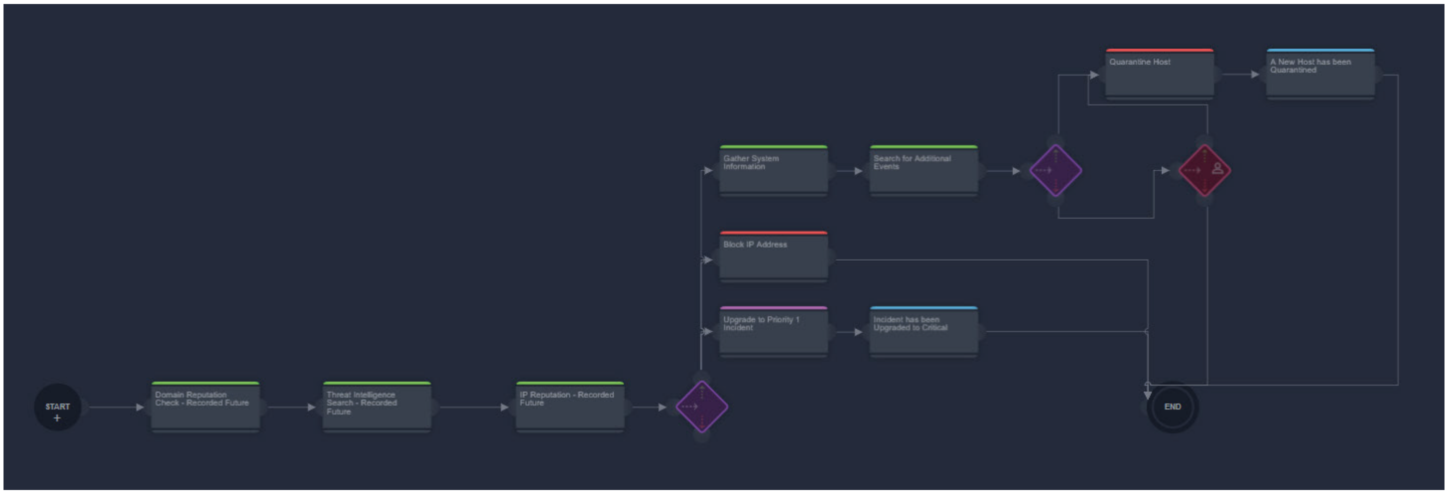
If any of the reputation checks report a threat score of 50 or above, the R3 Runbook will automatically change the priority of the incident to critical and will proceed to block the IP at the firewall and gather system information from the affected host. The system information is then checked against any additional events that may have been observed for that host over a pre-defined amount of time. If the affected host has been observed within any additional alerts, the R3 Runbook will pull all running processes on the host and will automatically quarantine it from the network. In the event the host must be quarantined, an email notification is sent out to the responsible team to indicate further action is necessary.

If the host has not been observed within any prior events, the R3 Runbook will issue a User Choice condition. This condition will temporarily pause the R3 Runbook and allow for an investigator to analyze the information gathered and determine whether the host should be quarantined or segmented for further observation.

## Recorded Future Actions

### Enrichment

- Threat Intelligence Search IP Reputation
- URL Reputation
- Domain Reputation
- File Reputation


START
Domain Reputation Check - Recorded Future
Threat Intelligence Search - Recorded Future
IP Reputation - Recorded Future
Gather System Information
Search for Additional Events
Block IP Address
Upgrade to Priority 1 Incident
Incident has been Upgraded to Critical
Quarantine Host
A New Host has been Quarantined
END

## About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.

www.recordedfuture.com @RecordedFuture

## About DFLabs

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 invest ment 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 www.dflabs.com or connect with us on Twitter @DFLabs.