

INTEGRATION BRIEF

DFLabs and Recorded Future: Simplifying Intelligence Gathering.

Combining industry-leading Threat Intelligence with Recorded Future with automation and orchestration excellence from DFLabs.

DFLABS.COM

Automate.
Orchestrate.
Measure.



| 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

utilize their time investigating an incident rather than focusing this valuable time performing manual information gathering and the data correlation necessary to prioritize an event.

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

| The Problem.

Cyber security 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 often times 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 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:

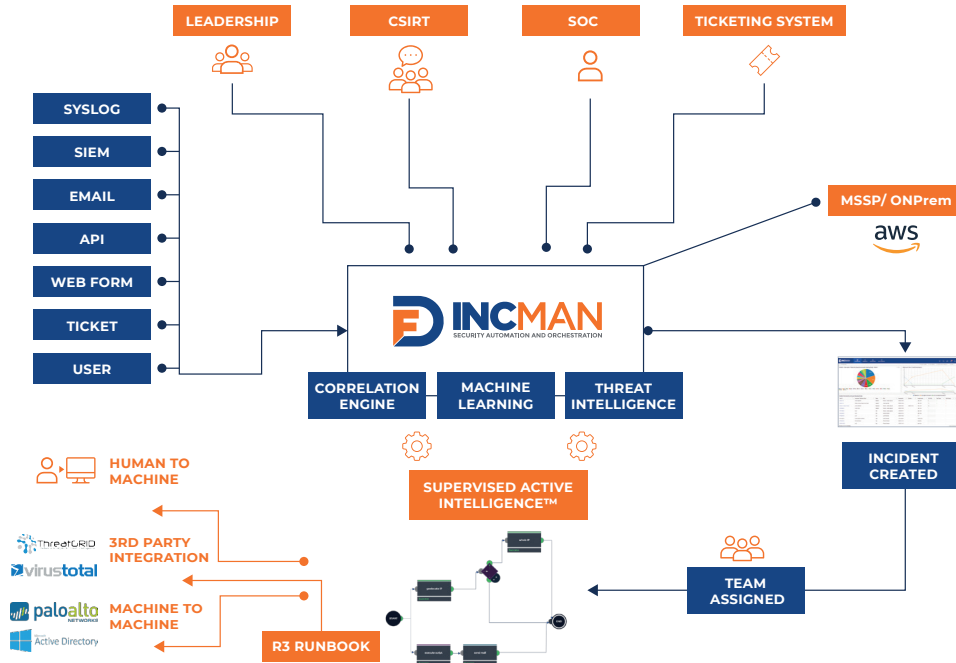
- What intelligence data should I use and how can I use it?
- How can I cut down the time necessary for a proper investigation?
- Where should my intelligence data be utilized?

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

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

**Automate.
Orchestrate.
Measure.**

DFLabs IncMan SOAR Overview.



About Recorded Future.

Recorded Future is an industry leading Threat Intelligence platform which 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 automates, orchestrates and measures 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% and increase incident handling by 300%.

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 utilized?

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%
- Maximize security analyst efficiency by 80%
- Increase the number of resolved

Automate.
Orchestrate.
Measure.

Use Case.

A WAF alert for a suspicious redirect is received and automatically triggers a new incident inside of IncMan SOAR. Utilizing 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 which 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.

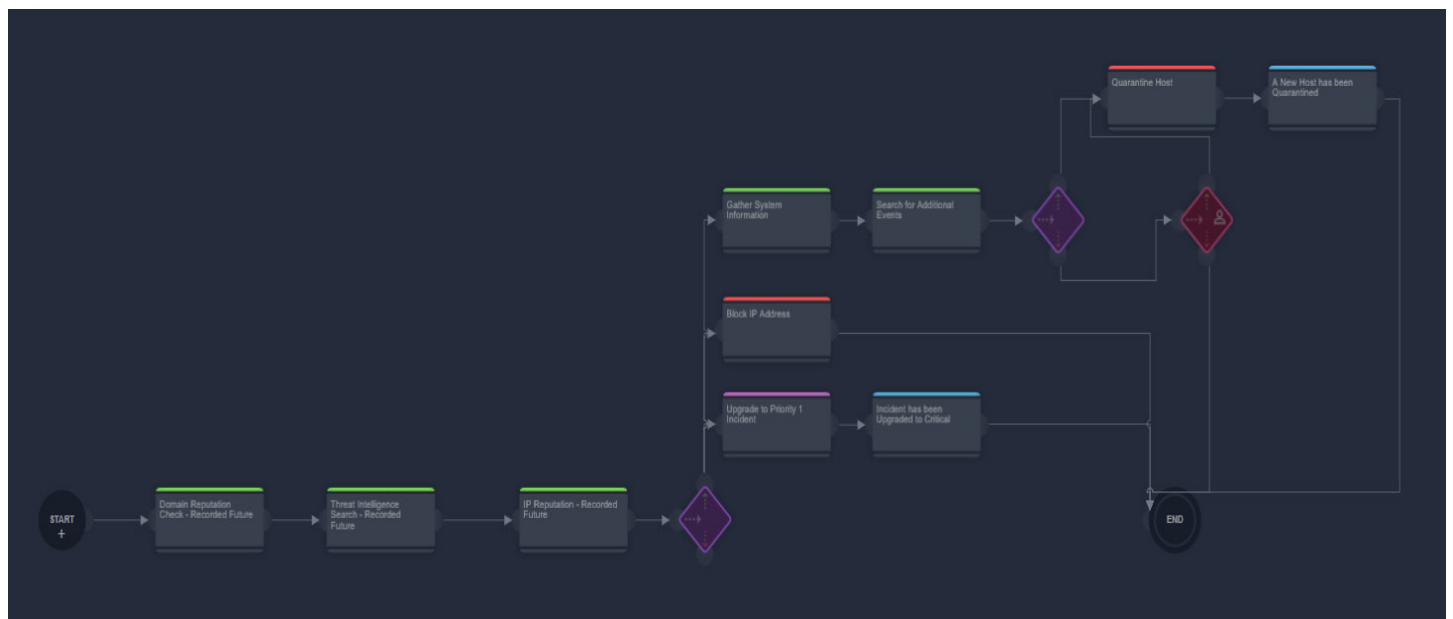
RECORDED FUTURE ACTIONS

Enrichment

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

LEARN MORE

For more information on how to take your incident response to the next level with DFLabs IncMan SOAR, contact your DFLabs representative or visit www.dflabs.com.



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 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 www.dflabs.com or connect with us on Twitter [@DFLabs](https://twitter.com/DFLabs).

CONTACT US

US – +1 201 579 0893

UK – +44 203 286 4193

IT – +39 037 832 416

E – sales@dflabs.com

About Recorded Future.

Recorded Future delivers the only complete threat intelligence solution powered by patented machine learning to lower risk. We empower organizations to reveal unknown threats before they impact business, and enable teams to respond to alerts 10 times faster.

To supercharge the efforts of security teams, our technology automatically collects and analyzes intelligence from technical, open web, and dark web sources and aggregates customer-proprietary data.

Recorded Future delivers more context than threat feeds, updates in real time so intelligence stays relevant, and centralizes information ready for human analysis, collaboration, and integration with security technologies.

91 percent of the Fortune 100 use Recorded Future.

Learn more at www.recordedfuture.com and follow us on Twitter at [@RecordedFuture](https://twitter.com/RecordedFuture).

Automate.
Orchestrate.
Measure.

