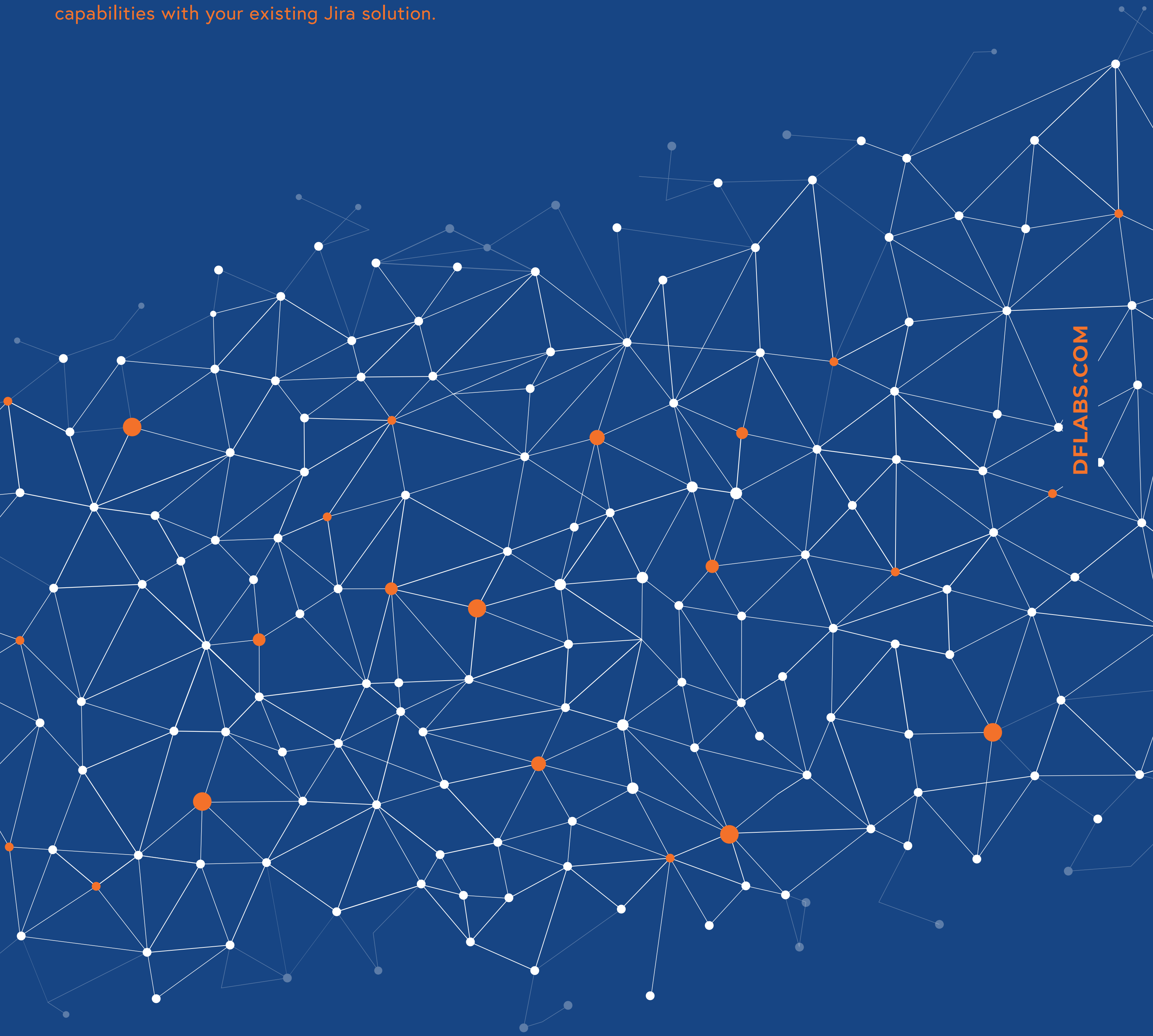
INTEGRATION BRIEF

DFLabs and Jira:

Streamline Incident Management and Issue Tracking.

Integrate IncMan SOAR's Orchestration, Automation and Response capabilities with your existing Jira solution.



DFLABS.COM

Automate.
Orchestrate.
Measure.

JIRA | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Combine the power of IncMan SOAR's Orchestration, Automation and Response capabilities with Jira's industry leading issue tracking software to manage your security incidents in a whole new and more efficient way.

IncMan's Rapid Response Runbooks (R^3 Runbooks) can be used to automatically create issues within Jira and continue to update the issue as the incident progresses. Bridge the gap between teams orchestrating incidents with IncMan and teams tracking other tasks with Jira to ensure that all teams maintain a holistic view of the incident and function as a single, unified body.

Security Operations Teams struggle to gain visibility of threat and rapidly respond to incidents.

The Problem.

Security incidents are complex and dynamic events, requiring the coordinated participation from multiple teams across the organization. For these teams to work with maximum efficiency, as a single body, it is critical that information flow seamlessly between all teams in real-time.

Faced with a continued onslaught of security incidents, organizations must find ways to maximize the utilization of their limited resources to remain ahead of the attackers and ensure the integrity of the organization's critical resources.

The DFLabs and Jira Solution.

Security Operations Teams struggle to gain visibility of threats and rapidly respond to incidents due to the sheer number of different security technologies they must maintain and manage and the resulting flood of alerts. Aggregating these into a single pane of glass to prioritize what is critical and needs immediate attention requires a platform that can consolidate disparate technologies and alerts, and provides a cohesive and comprehensive capability set to orchestrate incident response efforts.

By integrating with Jira, IncMan SOAR extends these capabilities to Jira users, combining the Orchestration, Automation and Response power of IncMan with the organization's existing issue tracking process.

DFLabs IncMan SOAR and Jira solve these specific challenges:

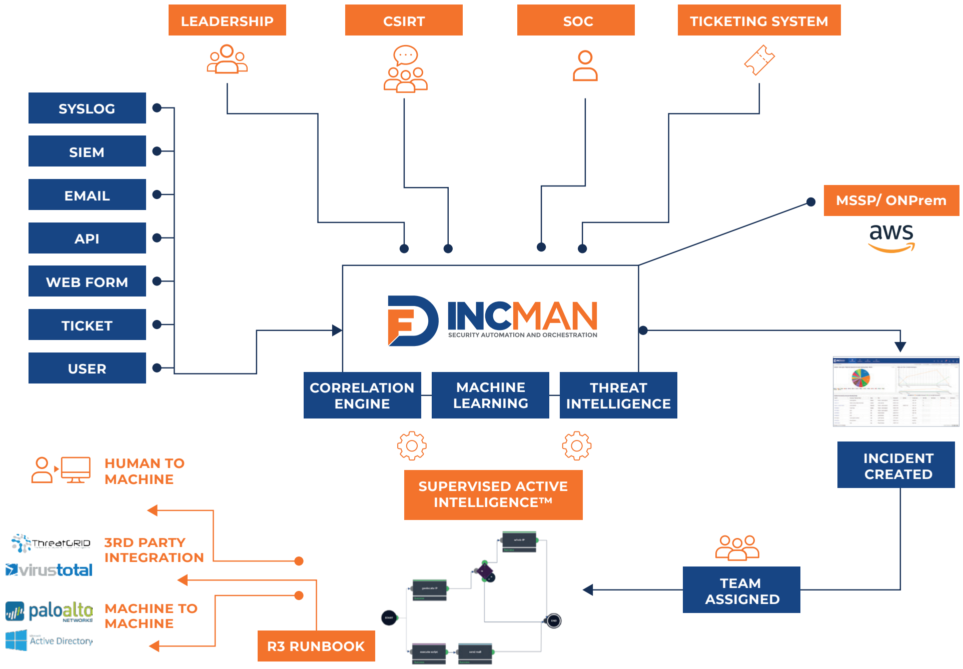
- How can I aggregate and correlate disparate security sources to increase my visibility of threats and effectively investigate alerts and incidents?
- How can I prioritize my response to security incidents at volume and at scale across a growing attack surface?
- How can I rapidly respond to security incidents with limited resources to contain damage and limit legal exposure?

Combining IncMan SOAR, Jira 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 Jira.

Jira's industry leading issue tracking solution has been battle-tested and become the core of organization's support, IT, incident response and project management processes worldwide. Jira allows teams from across the organization to collaborate and share information to plan, track and report projects and issues in real-time, maximizing efficiency and reducing impacts on the organization's critical business processes.

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 uses machine learning and Rapid Response Runbooks (R^3 Runbooks) as a force multiplier that has enabled security teams to reduce average incident resolution times by 90% and increase incident handling by 300%.

Automate.
Orchestrate.
Measure.

CHALLENGES

- How can I ensure that all teams have the most up-to-date incident information?
- How can I integrate the power of IncMan SOAR into my existing issue management process?
- How can I enable all teams to work as a single, unified body to increase the efficiency of the response process?
- How can I quickly communicate critical information to those outside the security team?

DFLABS AND JIRA SOLUTION

- Automatically create and update Jira issues using IncMan's R^3 Rapid Response Runbooks
- Share information seamlessly between solutions and teams
- Integrate with your existing issue management process

RESULTS

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

Use Case.

An alert of a host communicating with a potentially malicious domain has automatically generated an Incident within IncMan SOAR. This alert is automatically categorized within IncMan based on the organizations policies, which initiates the organization's Domain reputation runbook, shown below.

Through this runbook, IncMan automatically gathers domain reputation information for the domain which generated the alert. If the resulting domain reputation information indicates that the domain may be malicious, IncMan will use an Notification action to automatically create a new Issue within Jira, allowing Jira users to immediately begin next steps.

Next, using additional Enrichment actions, IncMan will automatically gather additional information regarding the suspicious domain, such as WHOIS and geolocation information. IncMan will then automatically update the Jira issue with this information. Finally, a screenshot of the page (if applicable), is taken and added to IncMan.

The automated workflow of IncMan's R^3 Runbooks means that an IncMan incident and Jira issue will have been automatically generated, and these enrichment actions through the Quick Integration Connector with Jira and other enrichment sources will have already been committed before an analyst is even aware that an incident has occurred.

Both IncMan and Jira users are now able to perform their respective tasks, knowing that they are each working with the same information, and can continue to do to as the incident progresses. Harnessing the power of Jira's industry leading issue tracking solution, along with the Orchestration, Automation and Response of DFLab's IncMan SOAR, organizations can elevate their incident response process, leading to faster and more effective response and reduced risk across the entire organization.

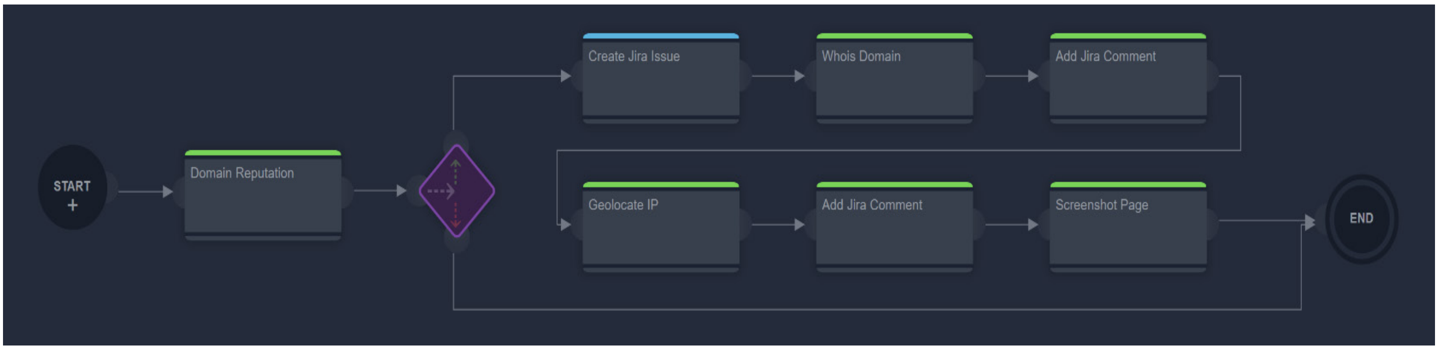
JIRA ACTIONS

Notifications

- ✓ Add comment to Issue
- ✓ Create Issue
- ✓ Delete Issue
- ✓ List Issue Status
- ✓ List Issue Types
- ✓ List Project
- ✓ Set Issue Status
- ✓ Update Issue

LEARN MORE

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



Automate.
Orchestrate.
Measure.

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.

CONTACT US

US – +1 201 579 0893
UK – +44 203 286 4193
IT – +39 037 832 416

E – sales@dflabs.com

About LogPoint.

LogPoint enables organizations to convert data into actionable intelligence, improving their cybersecurity posture and creating immediate business value.

Our advanced next-gen SIEM, UEBA and Automation and Incident Response solutions, simple licensing model, and market-leading support organization empower our customers to build, manage and effectively transform their businesses.

We provide cybersecurity automation and analytics that create contextual awareness to support security, compliance, operations, and business decisions.

Our offices are located throughout Europe and in North America.

Our passionate employees throughout the world are achieving outstanding results through consistent customer value-creation and process excellence.

With more than 50 certified partners, we are committed to ensuring our deployments exceed expectations.

For more information visit www.logpoint.com or connect with us on Twitter @LogPoint.

Automate.
Orchestrate.
Measure.

JIRA | DFLABS
CYBER INCIDENTS UNDER CONTROL