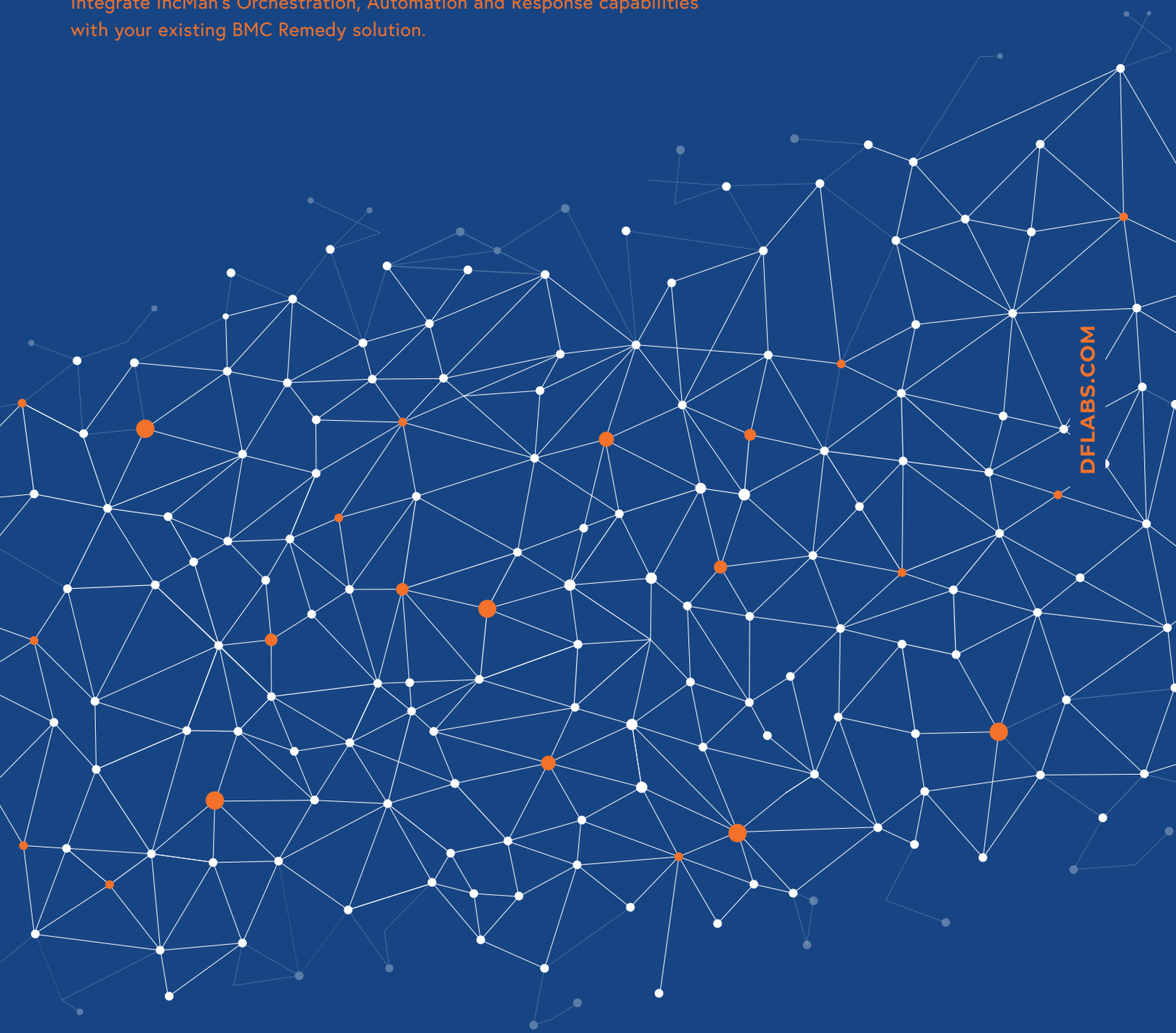
INTEGRATION BRIEF

DFLabs and BMC Remedy: Streamline Incident Management and Issue Tracking.

Integrate IncMan's Orchestration, Automation and Response capabilities with your existing BMC Remedy solution.



DFLABS.COM

Automate.
Orchestrate.
Measure.

bmc Remedy | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Security incidents are complex and dynamic events, requiring coordinated participation from multiple teams across the organization and seamless information flow between all teams in real-time. Different teams often use isolated solutions, making the sharing of information a difficult, manual process. Integrating the organization's issue tracking through BMC Remedy with DFLabs IncMan SOAR allows teams to aggregate these data sources into a single pane of glass to prioritize what is critical and needs immediate attention and requires a platform that can consolidate disparate technologies and alerts and provide a cohesive and comprehensive capability set to orchestrate incident response efforts.

Different teams often use isolated solutions, making the sharing of information a difficult, manual process.

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.

DFLABS.COM

The DFLabs and BMC Remedy 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 BMC Remedy, DFLabs IncMan extends these capabilities to Remedy users, combining the Orchestration, Automation and Response power of IncMan with the organization's existing issue tracking process.

DFLabs IncMan SOAR and BMC Remedy solve these specific challenges:

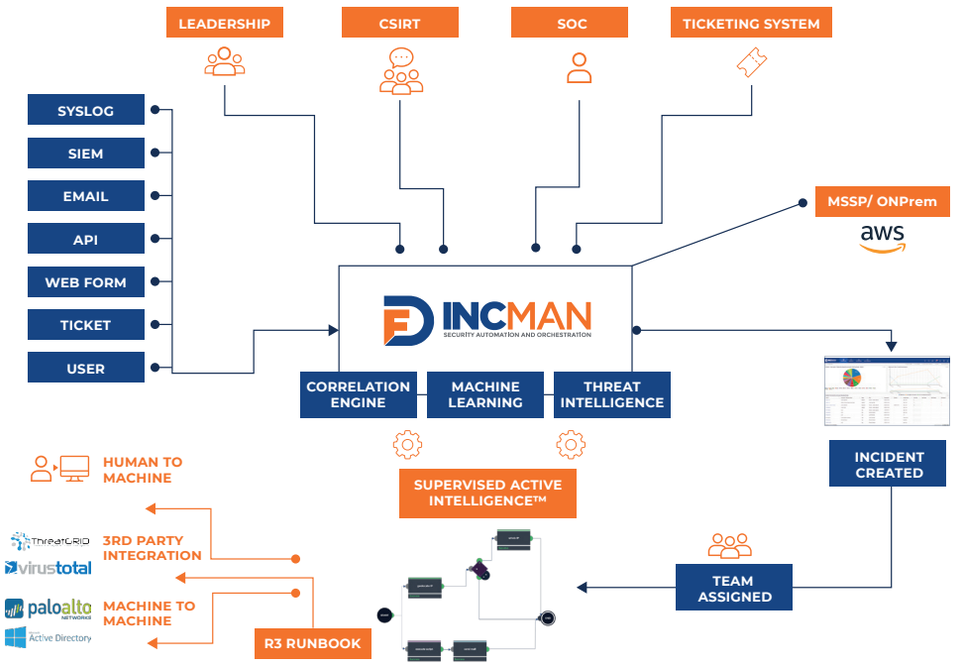
- How can I integrate the power of IncMan SOAR into my existing issue management process?
- How can I enable all teams to work as a single, unified body to increase the efficiency of the response process?
- How can I quickly communicate critical information to those outside the security team?

Combining IncMan SOAR, BMC Remedy 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 BMC Remedy.

BMC Remedy IT Service Management Suite (BMC Remedy ITSM Suite) provides out of-the-box IT Information Library (ITIL) service support functionality. BMC Remedy ITSM Suite streamlines and automates the processes around IT service desk, asset management, and change management operations. It also enables you to link your business services to your IT infrastructure to help you manage the impact of technology changes on business and business changes on technology - in real time and into the future. In addition, you can understand and optimize the user experience, balance current and future infrastructure investments, and view potential impact on the business by using a real-time service model.

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 (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 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 BMC REMEDY SOLUTION

- Integrate IncMan SOAR into the existing issue management process
- Enable separate teams to work as a single, unified body
- Communicate critical information and tasks outside the security team

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 BMC Remedy, allowing Remedy 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 BMC Remedy issue with this information. Finally, a screenshot of the page (if applicable), is taken and added to IncMan.

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

Both IncMan and BMC Remedy 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 BMC Remedy's industry leading issue tracking solution, along with the Orchestration, Automation and Response capabilities of DFLab's IncMan SOAR solution, organizations can elevate their incident response process, leading to faster and more effective response and reduced risk across the entire organization.

BMC REMEDY ACTIONS

Notification

- Add Workinfo to Ticket
- Create Ticket/Issue
- Close Ticket

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.

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 BMC.

BMC helps customers run and reinvent their businesses with open, scalable, and modular solutions to complex IT problems. Bringing both unmatched experience in optimization and limitless passion for innovation to technologies from mainframe to mobile to cloud and beyond, BMC helps more than 10,000 customers worldwide reinvent, grow, and build for the future success of their enterprises, including 92 of the Forbes Global 100.

Learn more at www.bmc.com and follow us on Twitter at @BMCSoftware.

Automate.
Orchestrate.
Measure.

bmc Remedy | DFLABS CYBER INCIDENTS UNDER CONTROL