INTEGRATION BRIEF

DFLabs and PagerDuty: Unify Operations for Effective Incident Response.

Integrate IncMan SOAR's automation capabilities with your existing PagerDuty solution to ensure critical information is provided to all relevant stakeholders during an incident.

DFLABS.COM

Automate.
Orchestrate.
Measure.

pagerduty | DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

The ability for an organization to operate in a unified fashion when responding to a potential security incident can be the difference between and incident and a full-blown breach. Each operational unit within a company will develop their own processes and procedures and it is vital that incident responders know what these processes and procedures are, and who needs to be involved in case of an incident.

DFLabs' integration with PagerDuty will help organizations bridge this gap by taking the complexity out of these differing policies to provide a unified plan of attack. With IncMan SOAR's automation power and PagerDuty's automatic workflow notification system, organizations can build their different policies and procedures into one seamless process. This allows incident responders to focus their time and efforts on containing a potential threat, confident that the appropriate stakeholders have been notified according to the organization's incident handling policies.

Each operational unit within a company will develop their own processes and procedures and it is vital that incident responders know what these are.

The Problem.

When investigating an active incident there are a lot of investigational processes and stakeholders to consider. Depending on the type of incident and its severity, security professionals may need the assistance of numerous departments outside of the security operations center.

The need to work in conjunction with these outside departments can make an incident responder's job even harder. Each department may have different policies and procedures and escalation processes which can cause a responder to waste valuable time trying to decipher. Escalations to an incorrect department or subject matter expert can cause potentially dangerous gaps in an organization's response.

DFLABS.COM

The DFLabs and PagerDuty 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 PagerDuty solve these specific challenges:

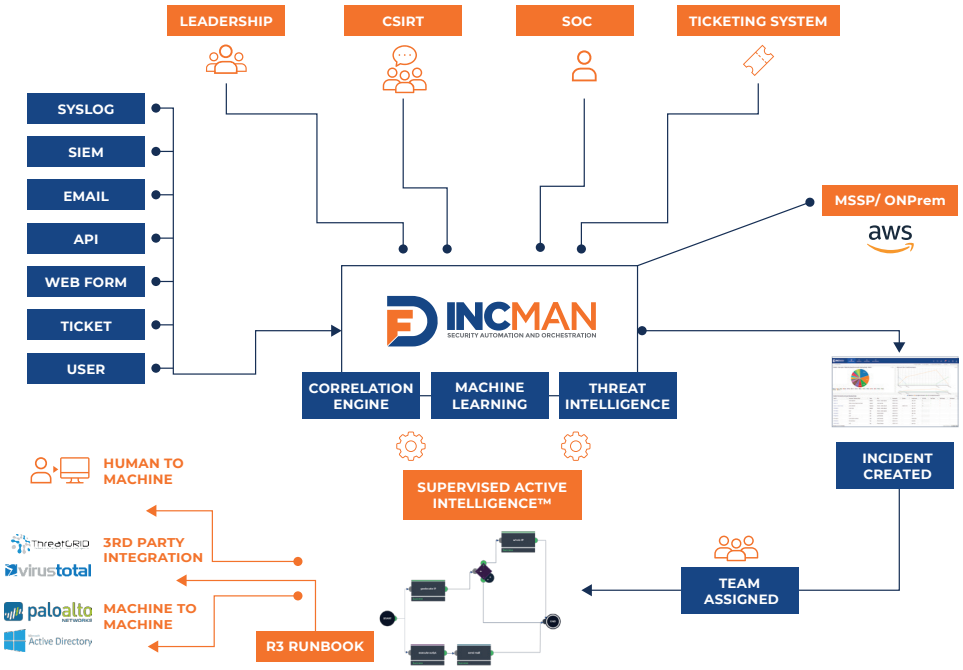
- How can all stakeholders be kept informed during an active incident?
- How can incident responders ensure all investigative processes are being followed?
- How can security incidents be escalated to the correct subject matter experts in a timely manner to provide the critical information necessary to contain a threat?

Combining IncMan SOAR, PagerDuty 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 PagerDuty.

PagerDuty is the leading digital operations management platform for businesses. PagerDuty's on-call management capabilities make it simple to distribute on-call responsibilities across all teams within an organization. PagerDuty helps to enforce accountability and quality as organizations onboard new services at scale with intuitive, flexible scheduling and escalation.

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 all stakeholders be kept informed during an active incident?
- How can incident responders ensure all investigative processes are being followed?
- How can security incidents be escalated to the correct subject matter experts in a timely manner to provide the critical information necessary to contain a threat?

DFLABS AND PAGERDUTY SOLUTION

- Rapidly relay incident and alert details to stakeholders outside of the SOC
- Build department specific processes into incident handling
- Gain confidence in alert and incident escalation processes by involving the correct subject matter experts at the first sign of an attack

RESULTS

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

Use Case.

A Data Loss Prevention (DLP) solution triggers an alert in IncMan SOAR to the presence of potentially sensitive data being uploaded to GitHub. The DevOps team regularly utilizes GitHub for hosting their projects, but the DLP solution has detected the potential presence of an API key within the uploaded code. IncMan receives the alert and begins to gather information on the user who executed the uploaded the code and downloads the file which was uploaded.

Once the file has been downloaded, IncMan reaches a User Choice decision, which pauses the automation and allows an analyst to review the previously gathered information. If the analyst finds that an API key was indeed present within the uploaded code and poses a risk to the organization, and the analyst may choose the User Choice path within IncMan which will cause a new incident to be created in PagerDuty. The raw output from the downloaded file will be added to the PagerDuty incident and a new responder request will be created. This request will follow the predetermined escalation processes agreed upon by the DevOps team.

An email will be sent to the DevOps team subject matter expert to begin scrubbing the sensitive data from the site. Once the email has been sent to the responsible party, IncMan will update the incident to include the assigned responder to the incident.

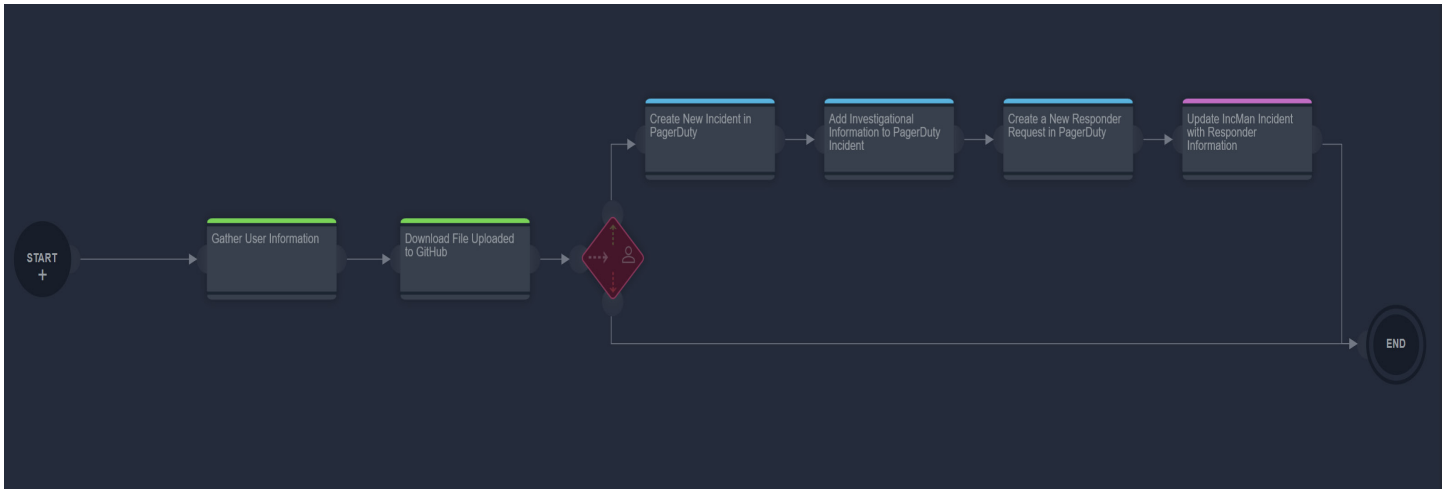
PAGERDUTY ACTIONS

Notification

- Add Comment to Incident
- Create Responder Request
- Get Alert Details
- Get Incident Details
- List Escalation Policies
- List Incident Alerts
- List Tickets
- List Priorities
- List Users
- Create Incident Status

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 PagerDuty.

PagerDuty is a leading digital operations management platform for organizations. Over 10,500 customers - including enterprises such as IBM, CE, Capital One, American Eagle Outfitters, Pitney Bowes, Box and ING - and small to midsize organizations around the world trust PagerDuty to improve digital operations, drive revenue, mitigate threats, protect assests, and delight customers.

To learn more visit www.pagerduty.com and follow us on Twitter at @PagerDuty.

Automate.
Orchestrate.
Measure.

pagerduty | DFLABS
CYBER INCIDENTS UNDER CONTROL