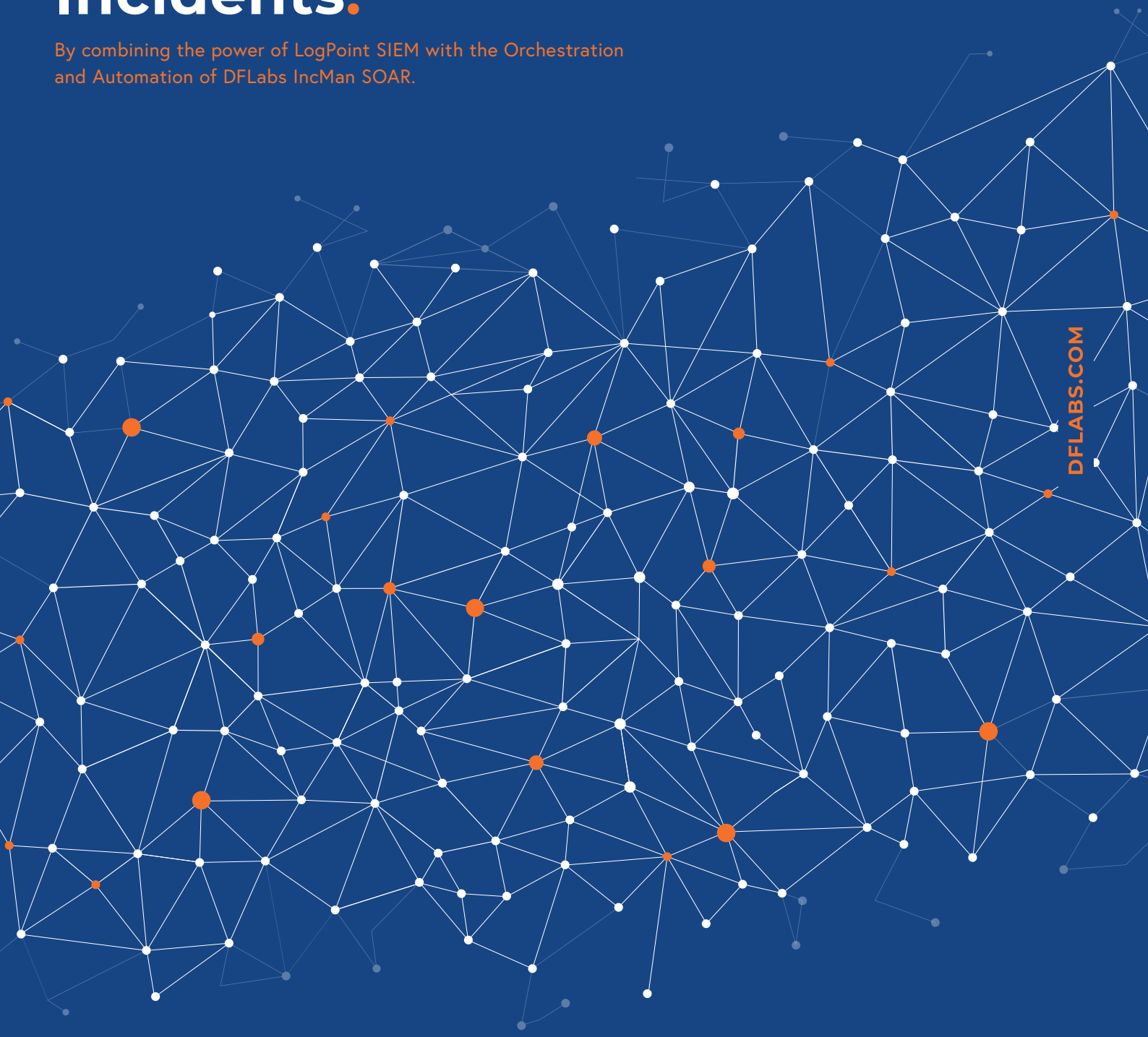
INTEGRATION BRIEF

DFLabs and LogPoint: Respond Faster and More Efficiently to Cyber Security Incidents.

By combining the power of LogPoint SIEM with the Orchestration and Automation of DFLabs IncMan SOAR.



Automate.
Orchestrate.
Measure.

LOGPOINT
Unified Simplicity

DFLABS
CYBER INCIDENTS UNDER CONTROL

Solution Overview.

Combine the power of LogPoint SIEM with the Orchestration, Automation and Response capabilities of DFLabs IncMan SOAR to respond faster and more efficiently to cyber security incidents.

Utilize LogPoint's native application to automatically push events to IncMan for automated Enrichment and Containment via IncMan's R^3 Rapid Response Runbooks.

Automatically query LogPoint via IncMan's R^3 Rapid Response Runbooks to gather additional intelligence for furtherautomated Enrichment and Containment actions.

Orchestration and Automation are critical components in responding effectively and efficiently to a cyber security incident.

The Problem.

Cyber security incidents are complex, potentially involving numerous assets being monitored by a myriad of different prevention and detection technologies. Investigating a cyber security incident requires the involvement of many different people, processes and technologies, all of which must work together seamlessly for an effective and efficient response. Failure to properly orchestrate these many moving parts can lead to increased risk, exposure and losses.

During a cyber security incident, context is key. Without proper context, analysts and managers are unable to make informed decisions regarding potential risk, containment and recovery. Providing this necessary context can be manual and time consuming, wasting valuable time as attackers continue to move throughout the network unobstructed.

DFLABS.COM

The DFLabs and LogPoint Solution.

Orchestration and Automation are critical components in responding effectively and efficiently to a cyber security incident. Combing the aggregation, storage and analytics power of LogPoint with the Orchestration, Automation and Response power of IncMan drastically multiplies the impact of the existing security program by removing the analyst from the repetitive, mundane tasks, allowing them to focus their time and energy where they can have the greatest impact.

Harnessing the power of both LogPoint and IncMan allows organizations of any size and vertical to drastically simplify their security operations program.

DFLabs IncMan and LogPoint solve these specific challenges:

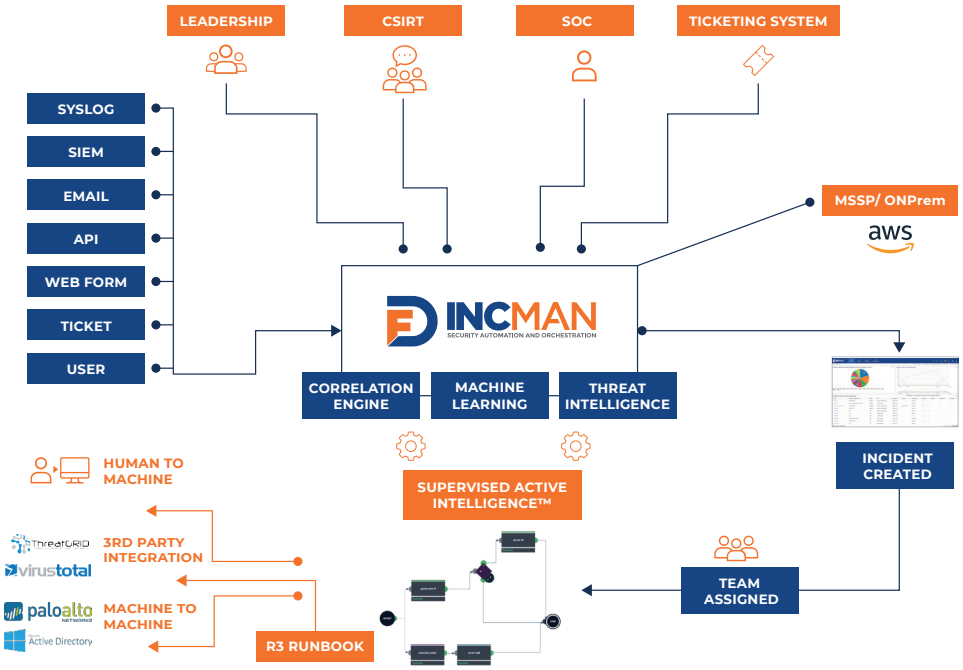
- How can I use my existing resources more effectively?
- How can I reduce the mean time to detection (MTTD)?
- How can I reduce the mean time to response (MTTR)?

Combining IncMan, LogPoint 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 LogPoint.

LogPoint is an industry leader in Next Generation SIEM solutions, achieving the highest rating in Gartner's Peer Insights evaluation, with a heavy emphasis on ease of use and scalability. LogPoint offers unique detection and response capabilities through an advanced analytics layer and broad common event taxonomy, allowing correlations to detect attacks and misuse across enterprise applications such as ERP, Cloud and custom-developed applications. With strong UEBA capabilities, advanced reporting features, a strong analytics layer and rich data visualization capabilities, LogPoint delivers best-of-breed solutions to today's security challenges.

About DFLabs IncMan.

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%.

CHALLENGES

- How can I use my existing resources more effectively?
- How can I reduce the mean time to detection (MTTD)?
- How can I reduce the mean time to response (MTTR)?

DFLABS AND LOGPOINT SOLUTION

- Automate repeatable, mundane tasks
- Orchestrate actions across multiple security tools
- Enrich raw data, allowing for more informed, effective decisions
- Reduce the mean time to detection and mean time to response, minimizing potential risk

RESULTS

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

Automate.
Orchestrate.
Measure.

Use Case.

A proxy has observed an internal host communicating with an IP address that LogPoint has enriched through dynamic threat intelligence enrichment, to be a known command and control server used by malicious actors. As the LogPoint correlation engine is activated, the event is enriched with GEO-IP information, correlated with assest management data to identify the owner of the device and the observation is cross-referenced with previously raised incidents. Once the initial triage and processing is done, LogPoint pushes the alert through the IncMan application directly into IncMan, which automatically generated an incident and initiated an automated response, including executing the R^3 Runbook shown below.

The runbook begins by performing several basic Enrichment actions, such as performing a Whois query and an IP geolocation search. These Enrichment actions are followed by a Containment action, which is used to block the malicious IP address at the perimeter firewall.

Once the initial IP address is blocked, an additional Enrichment action is used to query LogPoint for a list of all IP addresses the internal host has communicated with in the past 30 minutes. Next, an Enrichment action is used to query each of these IP addresses against the organization's threat reputation service of choice (for example, VirusTotal, Cisco Umbrella or McAfee ATD).

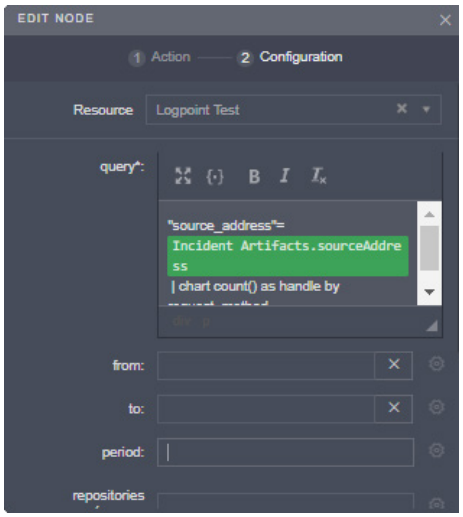
Any IP addresses which have a negative reputation will undergo a similar process to the initially identified malicious IP address; first utilizing several Enrichment actions to perform basic data enrichment, then being blocked at the perimeter firewall using a Containment action.

Once these IP addresses have been blocked to prevent any additional risk, LogPoint is again queried; this time for any other internal hosts which may have been communicating with these additional malicious IP addresses.

LogPoint leverages dynamic lists and enrichment capabilities to track entities and users associated with the breach and continuously monitor the environment in real time. As the attack progresses, additional data is added to the incident and forwarded to IncMan for further processing.

If any other internal hosts have been observed communicating with any of these additional malicious IP addresses, a final Enrichment action will be used to gather further information regarding each internal host from the IT asset inventory. This information will be automatically stored within the IncMan Incident and will be available for an analyst for review and follow up.

To ensure that each additionally potentially compromised internal host is further investigated by an analyst, a Notification action is used to immediately notify security team leaders about the identification of these additional potentially compromised hosts. If the organization were utilizing an IT ticketing system, an additional integration could be used to automatically generate an IT ticket to ensure additional accountability.



LOGPOINT ACTIONS

Enrichment

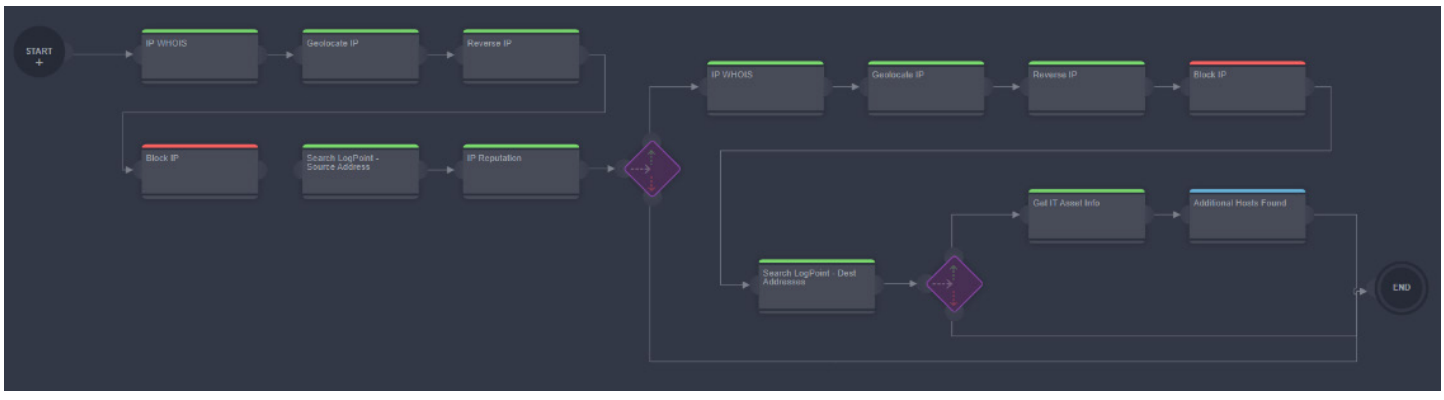
- Search Into Events

External

- Forward Events

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.

CONTACT US

DK – +45 7060 6100
DE – +49 89 8905 6730
FR – +33 1 80 88 50 20
NP – +977 1 55 41326
SE – +45 7060 6100
UK – +44 203 893 3003
US – +1 866 475 5431

E – info@logpoint.com

Automate.
Orchestrate.
Measure.

LOGPOINT
Unified Simplicity

DFLABS
CYBER INCIDENTS UNDER CONTROL